Umstrittene Partnerschaft: Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit

Bendiek, Annegret

Veröffentlichungsversion / Published Version
Forschungsbericht / research report

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

SWP-Studie
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale
Politik und Sicherheit

Annegret Bendiek

Umstrittene Partnerschaft

Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit

S 26
Dezember 2013
Berlin

SWP-Studien unterliegen einem Begutachtungsverfahren durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*. Sie geben ausschließlich die persönliche Auffassung der Autoren und Autorinnen wieder.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372

Inhalt

Dr. Annegret Bendiek ist stellvertretende Leiterin der Forschungsgruppe EU-Außenbeziehungen

Umstrittene Partnerschaft
Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit

Edward Snowdens Enthüllungen über die Spionagepraktiken des US-amerikanischen Nachrichtendienstes NSA haben in der europäischen und vor allem der deutschen Öffentlichkeit für viel Aufsehen gesorgt. Der engste politische Partner Europas hat in großem Stil private Kommunikation abgehört und nicht einmal davor Halt gemacht, Regierungsstellen der EU und ihrer Mitgliedstaaten heimlich zu belauschen. Die wichtigsten und alltäglich von Europäern angesteuerten Internetplattformen wie Google, Yahoo und Amazon wurden und werden von amerikanischen Regierungsstellen dazu benutzt, Informationen über europäische Bürger auf Wegen zu erhalten, die in fundamentalem Widerspruch zum europäischen Rechtsempfinden und zum Grundrecht auf informationelle Selbstbestimmung stehen. Viele befürchten, dass die transatlantische Partnerschaft zwischen Europa und den USA hierdurch großen Schaden und nicht wiedergutzumachende Vertrauensverluste erlitten hat. Manche Beobachter führen die transatlantischen Divergenzen in der Cyberpolitik auf die unterschiedliche geostrategische Positionierung der beiden Partner zurück und diagnostizieren letztlich unüberbrückbare Differenzen. Die USA seien in einem sehr viel höheren Maße als die EU global engagiert und sicherheitspolitisch herausgefordert. Insbesondere in der Cybersicherheitspolitik und immer mehr auch in der Frage der Internet Governance werde sich daher auch längerfristig kein Kompromiss zwischen »Venus Europa« und »Mars Amerika« erzielen lassen.

Die transatlantische Cyberpartnerschaft steht allerdings – trotz aller aktuellen Streitigkeiten – nach wie vor auf einem soliden normativen und institutionellen Fundament. Beide Seiten teilen grundlegende Prinzipien zum Umgang mit dem Internet. Sie sind davon überzeugt, dass alle Menschen freien Zugang zum Internet haben müssen und dass das Netz für Demokratie und Marktwirtschaft sowie die Zukunft der liberalen Ordnung außerordentlich nützlich ist. Einig sind sich beide Seiten auch darüber, dass es effektiver Mittel bedarf, um Schadsoftware zu limitieren, Kriminalität zu bekämpfen und kritische Infrastrukturen zu sichern.

Die Debatte über die Spionagepraktiken der NSA hat zwar deutlich gemacht, dass die USA und Europa unterschiedliche Auffassungen darüber haben, welches die angemessenen Mittel und Wege zur Umsetzung der gemeinsamen Ziele sind und wie mit normativen Spannungen umgegangen werden sollte. Doch der Streit darf nicht überbewertet und schon gar nicht als Bedrohung der transatlantischen Partnerschaft interpretiert werden. Die transatlantischen Dissonanzen sollten vielmehr zügig politisch bearbeitet werden. Drei größere Problemfelder sind hierbei zu berücksichtigen.

Global: Der bestehende Regulationsmodus für das Internet bindet die aufstrebenden Mächte Brasilien, Indien, China und Russland nicht ausreichend ein und ist zu einseitig auf die USA ausgerichtet. Der Begriff der Multistakeholder-Governance verdeckt, dass US-Interessen und US-Unternehmen faktisch die wichtigsten Agenda-Setter sind und finanziell schwächere Akteure nur geringe Chancen haben, sich in maßgeblichen Institutionen wie der Internet Corporation for Assigned Names and Numbers (ICANN) oder dem Internet Governance Forum (IGF) durchzusetzen. Lange Zeit haben die USA und Europa hier an einem Strang gezogen und das existierende Modell verteidigt. Die aktuellen Enthüllungen über US-amerikanische Abhörpraktiken haben in Europa jedoch wachsende Skepsis an diesem Modell erzeugt.

Transatlantisch: Was die militärisch-nachrichtendienstliche Cybersicherheitspolitik betrifft, besteht zwischen EU und USA ein tiefer Graben. Während die USA immer stärker auf Abschreckung und Offensive setzen, verfolgen die Europäer einen eher polizeilich ausgerichteten Ansatz, der den Aufbau von Widerstandsfähigkeit zum Ziel hat. Aus diesem Grund unterscheiden sich sowohl die Aufgaben- und Kompetenzzuweisung an die jeweiligen Nachrichtendienste als auch der Umgang mit bürgerlichen Grundrechten wie dem Recht auf informationelle Selbstbestimmung. Damit diese Differenz nicht in einen massiven Konflikt ausartet, müssen beide Seiten deutlich mehr Bereitschaft zeigen, auf den anderen zuzugehen. Eine wesentliche Bedingung für erfolgreiche Gespräche ist dabei, dass Amerikaner wie Europäer die innenpolitischen Grenzen transatlantischer Kompromissbereitschaft als Tatsache anerkennen. Solange die USA als globale Ordnungsmacht auftreten, werden sicherheitspolitische Aspekte und damit die Abschreckungsdimension von Cyberpolitik für sie weiterhin an erster Stelle stehen. Für die EU wiederum gilt, dass ihr Schwerpunkt auf der Abwehrbereitschaft (resilience) und Cyberkriminalitätsbekämpfung liegt und Fragen des Datenschutzes von überragender Bedeutung bleiben werden. Nur wenn beide Seiten diese Grenzen der Kooperation respektieren, ist eine wechselseitig gewinnbringende Zusammenarbeit in der globalen Cyberpolitik möglich.

Transnational: Die transatlantische Cyberpartnerschaft sieht sich einer ganzen Reihe neuer transnationaler Konflikte gegenüber, die dringend angegangen werden müssen. Zudem wurde auf der gesellschaftlichen Ebene viel Vertrauen zerstört. Die Enthüllungen haben die Bürger für die Kehrseite der Digitalisierung sensibilisiert. Es steht zu befürchten, dass viele Menschen das Internet nicht länger für sicher halten und mit zunehmender Skepsis und verstärkten Forderungen nach einer Renationalisierung von Kommunikationsstrukturen reagieren werden. Mit Blick auf die Verhandlungen über das Transatlantische Freihandels- und Investitionsabkommen (Transatlantic Trade and Investment Partnership, TTIP) wird schon heute verlangt, supranationale Rechtsinstrumente und unabhängige Streitschlichtungsgremien zu schaffen. Nicht nur die europäischen Mitgliedstaaten, sondern auch die USA werden sich aller Voraussicht nach mit dem Gedanken anfreunden müssen, dass Schwellenländer wie Brasilien, Indien, Südafrika und Indonesien verstärkt multilaterale Vereinbarungen in der Internet Governance einfordern werden, aber gleichwohl am Multistakeholder-Prozess festhalten wollen.

Transatlantische Prinzipien und Initiativen

Die EU und die USA haben im Laufe der letzten Jahre eine enge transatlantische Cyberpartnerschaft entwickelt.* Die Cyberpolitiken der beiden Räume stehen auf einem gemeinsamen normativen Fundament, gekennzeichnet durch übereinstimmende konzeptionelle Grundlagen und regulative Prinzipien sowie recht ähnliche innenpolitische Debatten. Diese grundsätzlichen Gemeinsamkeiten finden ihren Ausdruck zudem in vergleichbaren Vorstellungen über die angemessene Regelungsstruktur des Internet.[1]

Weil das Internet den gesamten Globus umspannt, ist die Partnerschaft in ihrem Gestaltungsanspruch nicht auf den transatlantischen Raum beschränkt, sondern umfasst »alle auf Datenebene vernetzten IT-Systeme im globalen Maßstab«.[2] Sowohl die USA als auch die Mitgliedstaaten der EU sind Dienstleistungsökonomien, die einen Großteil ihrer wirtschaftlichen Aktivität über das Internet abwickeln. Die wichtigsten Infrastrukturen, einschließlich der Energieversorgung, des Gesundheitssystems und des Transportwesens, hängen von stabilen Kommunikationswegen ab.[3]

Darüber hinaus ist die Internetnutzung in beiden Wirtschaftsräumen in den letzten Jahren rasant angestiegen und übertrifft diejenige in anderen Regionen der Welt bei weitem. In Europa sind heute ungefähr 75 Prozent aller Haushalte an das Internet angebunden, in Nord- und Südamerika immerhin 61 Prozent.[4] Bei der Entwicklung einer einheitlichen »Cyberraumpolitik« orientiert sich die EU an der amerikanischen International Strategy for Cyberspace vom Mai 2011. Gemeinsam mit internationalen Partnern und Organisationen, dem Privatsektor und der Zivilgesellschaft will die EU auf »die Bewahrung eines offenen, freien und sicheren Cyberraums« hinwirken und sich um »die Überbrückung der ›digitalen Kluft‹« bemühen.[5]

Multistakeholder-Modell

Die wohl wichtigste Gemeinsamkeit der Cyberpolitiken in USA und EU ist die Einsicht, dass das globale Internet als Gemeingut zu betrachten ist, das von der Idee der Freiheit geprägt ist.[6] Bürger sollen das Internet im größtmöglichen Ausmaß nutzen können und nur dort beschränkt werden, wo ihr Handeln anderen Schaden zufügt. Das Internet soll zudem den jeweiligen nationalen Gesetzen nur insoweit unterstehen, als Leitungen und Computer sich innerhalb nationaler Grenzen befinden.

* Ein ganz besonderer Dank gilt dem German Marshall Fund of the United States in Washington, der mich als Gastwissenschaftlerin herzlich aufgenommen und bei meinen Recherchen unterstützt hat.

1 Das Wort »Cyber« leitet sich aus dem altgriechischen »kybérnesis« ab und bedeutete ursprünglich die Steuerkunst des Seefahrers. Der US-amerikanische Mathematiker Norbert Wiener bezog den Begriff als Erster auf Datenverarbeitung und gilt als Begründer der Kybernetik. Diese Bezeichnung prägte er in seinem 1948 erschienenen Buch »Cybernetics: or Control and Communication in the Animal and the Machine«. Merkmale des Cyberraums sind Anonymität, komplexe Technik, Verwendung von Internettechnologie, fehlende Landesgrenzen, fehlende einheitliche Rechtsgrundlagen und fehlende einheitliche Sicherheits- und Qualitätsstandards. Vgl. Andreas Fröhling, »Was ist Cyberdefence?«, in: *Behörden Spiegel*, März 2013, S. 70.

2 Bundesministerium des Innern, *Cyber-Sicherheitsstrategie für Deutschland*, Berlin, Februar 2011, S. 14.

3 Nach Schätzungen der Boston Consulting Group hat die Webwirtschaft 2010 einschließlich des Onlinehandels und des Geschäfts zwischen Firmen mit 2,3 Billionen Dollar mehr Wert erzeugt als die Volkswirtschaften Italiens und Brasiliens zusammen. Bis 2016 sollen es 4,2 Billionen Dollar sein, mehr als die Wirtschaftsleistung Deutschlands. Vgl. Stephan Bauer/Klaus Schachinger, »Amazon, Google & Co.: Zeitenwende im Internet«, in: *Euro am Sonntag*, (19.6.2013) 24, S. 11.

4 Heute sind mehr als zwei Milliarden Menschen online. In den kommenden Jahren soll sich die Zahl verdoppeln. Vgl. International Telecommunication Union (ITU), *Facts and Figures. The World in 2013*, Genf 2013.

5 Vgl. Annegret Bendiek/Marcel Dickow/Jens Meyer, *Europäische Außenpolitik und das Netz. Orientierungspunkte für eine Cyber-Außenpolitik der EU*, Berlin: Stiftung Wissenschaft und Politik, Oktober 2012 (SWP-Aktuell 60/2012).

6 Freedom House weist aber auch darauf hin, dass vor allem in Indien, Brasilien, Venezuela und den USA der Grad der Freiheit im Internet deutlich geringer eingeschätzt wird als im Vorjahr. Das liegt vor allem an den Snowden-Enthüllungen, vgl. Freedom House, *Freedom on the Net 2013*, Washington, D.C./New York 2013, <www.freedomhouse.org/report/freedom-net/freedom-net-2013>; siehe auch »Russischer Geheimdienst will komplette Internetkommunikation speichern«, in: *Spiegel Online*, 21.10.2013.

Diese von beiden Seiten geteilten normativen Prinzipien der transatlantischen Cyberpartnerschaft finden ihren Ausdruck in einer weitgehend übereinstimmenden Vorstellung über die angemessene Regulierung des Internet. Im Rahmen des VN-Weltgipfels zur Informationsgesellschaft (World Summit on the Information Society, WSIS) entwickelte sich in den Jahren 2002 bis 2005 eine Debatte zwischen China und USA, ob das Internet staatlich oder privatwirtschaftlich verwaltet werden sollte. Als Antwort auf diese Frage erarbeitete eine vom damaligen VN-Generalsekretär Kofi Annan eingesetzte Working Group on Internet Governance (WGIG) das sogenannte Multistakeholder-Modell. Es wurde damals von 190 Staaten unterstützt und folgt der Idee, dass das Internet keine zentrale politische Instanz kennt, sondern auf dem Zusammenwirken aller beteiligten und betroffenen Stakeholder – Regierungen, Privatwirtschaft, Zivilgesellschaft und technische Community – beruht. Grundsätzlich kann jeder bei den wichtigsten regulativen Instanzen wie der Internet Society (ISOC), der Internet Engineering Task Force (IETF) oder dem Internet Governance Forum (IGF) mitarbeiten. Die Eintrittskarte ist »kein politisches Bekenntnis, sondern die Fähigkeit und Bereitschaft, etwas zur Lösung von praktischen (Internet-)Problemen beitragen zu können«.[7] Nicht die Herkunft oder die Zugehörigkeit zu einer Wählerschaft, sondern die Stärke des Arguments, die Innovationskraft eines Vorschlags und die Plausibilität von Bedenken sollen das Ergebnis bestimmen. Ein grober Konsens (»rough consensus«) gilt dann als erreicht, wenn es keine fundamentalen Einwände von wesentlichen beteiligten Gruppen mehr gibt.

Das von der Internet Corporation for Assigned Names and Numbers (ICANN)[8] verabschiedete neue Programm »generic Top Level Domain« (gTLD) ist ein Beispiel dafür, dass politische wie wirtschaftliche Probleme in einem Multistakeholder-Prozess gelöst werden können. Als schlagendstes Argument für die bestehende Multistakeholder-Struktur gilt ihr Erfolg in der Vergangenheit: Die Zahl der Internetnutzer hat sich binnen 20 Jahren auf rund zwei Milliarden erhöht. Die Offenheit des Internet hat innovative und kreative Applikationen hervorgebracht, die dem Netz seine kulturelle Vielfalt und wirtschaftliche Leistungsfähigkeit geben.[9]

Die bestehende Struktur ist allerdings nicht unumstritten. Vor allem autoritär regierte Staaten wie China, Russland und der Iran drängen auf eine direkter an die Vereinten Nationen gebundene Ordnung, in der die Regierungen wieder eine deutlich weitreichendere Kompetenz zur Regulierung erhalten. Eine breite westliche Allianz, bestehend aus den USA, den Mitgliedstaaten der EU, Japan, Australien und Kanada, weist solche Vorstöße allerdings bisher zurück. Befürchtet wird vor allem, eine stärkere Rolle von VN-Gremien würde die Gefahr des staatlichen Machtmissbrauchs erhöhen. Würde das Domain Name System (DNS) beispielsweise nicht mehr von ICANN, sondern von Regierungen im Rahmen der International Telecommunication Union (ITU) gesteuert, könnte es als politisches Machtinstrument verwandt werden, mit dessen Hilfe missliebigen Nutzern der Zugang zum Internet gesperrt werden kann. Die Great Firewall der chinesischen Regierung und die Blockade von Webseiten wie Google im Halal-Netz des Iran zeigen, dass dies eine nicht nur hypothetische Gefahr ist.[10]

Die Mitglieder der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Co-operation and Development, OECD) sehen dagegen die derzeitige Internet-Governance-Ordnung als neutrales Arrangement. So forderte der US-Kongress in einer Resolution, das existierende Modell der Internet Governance zu erhalten, und sprach sich gegen jede Ausweitung der ITU-Kompetenzen auf das Internet aus.[11] Auch das Europäische Parlament (EP) und die Kommission setzten sich anlässlich der World Conference on International Telecommunications (WCIT) 2012 in Dubai für den Erhalt eines offenen und freien Internet ein.[12]

7 Wolfgang Kleinwächter (Hg.), *Internet und Demokratie*, Berlin, Juni 2013 (MIND [Multistakeholder Internet Dialog] #5; Collaboratory Discussion Paper Series, Nr. 1), S. 8.

8 ICANN ist eine private Organisation, die die wahrscheinlich einzige zentrale Einrichtung des Internet verwaltet: das Domain Name System (DNS). Es legt fest, wie Internetadressen in IP-Adressen übersetzt werden. Das DNS besteht aus weltweit 13 Root-Name-Servern, von denen die meisten in den USA stehen. Sie bilden die zentrale Anlaufstelle für den Austausch von IP-Adressen.

9 Vgl. Vint Cerf, »Reflections about the Internet and Human Rights: Video Keynote«, in: Lorena Jaume-Palasi/Wolfgang Kleinwächter (Hg.), *Keep the Internet Free, Open and Secure*, Berlin 2013, S. 40f.

10 Vgl. Alex Comninos, *Freedom of Peaceful Assembly and Freedom of Association and the Internet*, Melville (Südafrika): Association for Progressive Communications (APC), Juni 2012.

11 Gautham Nagesh, »An Internet (Almost) Free from Government Control«, *Roll Call*, 17.4.2013, <www.rollcall.com/news/an_internet_almost_free_from_government_control-224101-1.html>.

12 European Commission, *Digital Agenda: EU Defends Open Internet at Dubai International Telecommunications Conference*,

Befürworter wie Gegner der bestehenden Multistakeholder-Struktur wissen jedoch, dass sie Governancefragen aufwirft, die noch nicht beantwortet sind. Die heftigen Debatten um das Thema Internetregulierung bei der ITU und um die Einführung neuer Top-Level-Domains bei ICANN zeigen, welche Bedeutung technische Standardisierung als politisches Instrument erlangt. Die Rolle nationaler wie auch supranationaler politischer Instanzen in diesen Gremien ist alles andere als verbindlich geklärt. Ihr Einfluss ist hier jedenfalls geringer als im amerikanischen oder europäischen Hoheitsgebiet. Noch heikler wird es, wenn einzelne technische Gatekeeper selbst zur Standardisierungsinstanz werden, wie dies beispielsweise im Browsermarkt zu beobachten ist.[13]

Innenpolitische Debatten

Innenpolitische Debatten, die in EU und USA über Cyberpolitik geführt werden, ähneln sich ebenfalls stark. Auf beiden Seiten des Atlantiks wird darüber diskutiert, wie ein möglichst barrierefreier Zugang zu digitalen Infrastrukturen sowohl in der Fläche als auch in der Geschwindigkeit des Zugangs (Breitbandinfrastruktur) erreicht werden kann und welche Beschränkungen legitim sind.[14] Die Europäische Kommission hat hierzu im Dezember 2012 eine »digitale Aufgabenliste« vorgelegt. Die oberste Priorität für die digitale Wirtschaft sieht die Kommission in einem stabilen regulatorischen Umfeld für Investitionen in Breitbandnetze. Seit Anfang Januar 2013 sind die neuen »Leitlinien der EU für die Anwendung der Vorschriften über staatliche Beihilfen im Zusammenhang mit dem schnellen Breitbandausbau« in Kraft.[15] Gestärkt werden soll ein diskriminierungsfreier Netzzugang (sogenannter Open Access), um den Wettbewerb in öffentlich geförderten Netzinfrastrukturen zu erleichtern.[16]

In USA und EU gleichermaßen umstritten ist zudem die Frage der Neutralität des Netzes. Die US-Regulierungsbehörde Federal Communications Commission (FCC) hatte 2010 eine Bestimmung erlassen, die es Providern untersagte, beim Transport von Internetpaketen nach Inhalten zu diskriminieren. Hiergegen ist eine Klage mit offenem Ausgang anhängig. Auch in Europa wird zurzeit diskutiert, ob Internetprovider gegen Zahlung Daten ausgewählter Inhalteanbieter (wie Facebook, YouTube oder Spotify) bevorzugt zu ihren Kunden transportieren dürfen. Mitte September 2013 hat die für die Digitale Agenda zuständige EU-Kommissarin Neelie Kroes eine Verordnung eingebracht, mit der europaweit ein Zwei-Klassen-Netz eingeführt werden soll.[17] Eine endgültige Festlegung zur Netzneutralität steht derzeit (Mitte Dezember 2013) allerdings noch aus.

Das Prinzip eines grundsätzlich möglichst unlimitierten Zugangs zum Internet schlägt sich auf beiden Seiten des Atlantiks in den sogenannten Freedom-Online-Strategien nieder.[18] Im Mai 2009 haben die USA[19] und dann im August 2012 die EU[20] jeweils Programme für die Internetfreiheit ins Leben gerufen.[21]

Memo/12/922, Brüssel, 30.11.2012; European Parliament, *Resolution on the Forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunication Union, and the Possible Expansion of the Scope of International Telecommunication Regulations*, 2012/2881(RSP), Straßburg, 22.11.2012.

13 Vgl. Guido Brinkel, »Datenpolitik«, in: Ansgar Baums/Ben Scott (Hg.), *Kompendium Digitale Standortpolitik*, Berlin, Juni 2013, S. 128–138 (133ff), <www.stiftung-nv.de/mstream.ashx?g=111327&a=1&ts=635215654714766229&s=&r=-1&id=151668&lp=635076896901470000>.

14 Strittig ist, ob ein Breitband-Universaldienst vorgeschrieben werden soll und ob Unternehmen verpflichtet werden können, die Infrastruktur bereitzustellen. In Deutschland beherrschen im Grunde zwei Unternehmen den Kabelmarkt: Kabel Deutschland und die US-Firma Liberty Global. Wolfgang Ehrensberger, »Begehrte Netze«, in: *Euro am Sonntag*, (19.6.2013) 24, S. 19.

15 *Amtsblatt der Europäischen Union*, 2013/C 25/01, 26.1.2013.

16 Hierbei ist zu erwähnen, dass Technologien des chinesischen Konzerns Huawei, global agierender Anbieter von Informationstechnologie und Telekommunikationslösungen, von mehr als 400 Telekommunikationsbetreibern in über 140 Ländern angewendet werden. Unter diesen befinden sich 45 der 50 weltweit größten Telekommunikationsanbieter. Huawei errichtet acht der neuen weltweit größten nationalen Breitbandnetze, darunter in Großbritannien, Neuseeland, Singapur und Malaysia. »Huawei will Engagement beim Netzausbau ausweiten«, in: *Behörden Spiegel*, Juli 2012, S. 19.

17 European Commission, *Commission Adopts Regulatory Proposals for a Connected Continent*, Memo/13/779, Brüssel, 11.9.2013.

18 Richard Fontaine/Will Rogers, *Internet Freedom. A Foreign Policy Imperative in the Digital Age*, Washington, D.C.: Center for a New American Security, Juni 2011.

19 Siehe hierzu U.S. Department of State, *21st Century Statecraft*, Mai 2009; vgl. auch Hillary Clinton, *Remarks on Internet Freedom*, Washington, D.C.: U.S. Department of State, 21.1.2010. Vgl. Fontaine/Rogers (Hg.), *Internet Freedom* [wie Fn. 18], S. 11–13.

20 Vgl. »European Parliament Calls for Digital Freedom«, in: *Bulletin Quotidien Europe*, (12.12.2012) 10749; European Parliament, *Draft Report on a Digital Freedom Strategy in EU Foreign Policy*, 2012/2094 (INI), Straßburg, 24.8.2012.

21 Vgl. Ben Wagner, »Freedom of Expression on the Internet: Implications for Foreign Policy«, in: *Global Information Society*

Die USA investierten bereits 2012 über 100 Millionen Dollar, um mit »Internet aus dem Koffer« Oppositionellen in Ländern mit autoritären Regimen einen ungehinderten Netzzugang zu sichern. Damit soll erreicht werden, dass Machthaber das Internet nicht mehr einfach abschalten können und dass Regimegegner sich im Konfliktfall auch weiterhin über soziale Netzwerke koordinieren und die Weltöffentlichkeit informieren können. Unter dem Eindruck der arabischen Umbrüche schmiedeten die USA 2011 mit Außenministerin Hillary Clinton an der Spitze die »Freedom Online Coalition«, der inzwischen 19 Staaten angehören.[22] Auch die Koalition möchte gewährleisten, dass politische Aktivisten in autoritären Staaten das Internet ohne Schwierigkeiten nutzen können. Mit der »No disconnect«-Strategie will auch die EU Menschenrechte und Grundfreiheiten sowohl online als auch offline wahren und das Internet und die Informations- und Kommunikationstechnik zugunsten politischer Freiheit, demokratischer Entwicklung und wirtschaftlichen Wachstums ausbauen.[23] Die EU kann hierfür mit dem neu geschaffenen Demokratiefonds Finanzierungen ermöglichen.[24]

Cyberkriminalität und die Budapester Konvention

Trotz weiterbestehender Divergenzen in der inhaltlichen Bestimmung und der Verwendung militärischer Begriffe wie »Cyberkrieg« hat sich ein gemeinsamer Grundkorpus an wichtigen Unterscheidungen und Kategorisierungen entwickelt.[25] Die Cyberkriminalität hat sich in den letzten Jahren auf beiden Seiten des Atlantiks massiv ausgeweitet.[26] Sie kostet ein deutsches Unternehmen im Schnitt 4,8 Millionen Euro im Jahr. Diese Zahl liegt zwar unter dem für die USA ermittelten Wert von 6,9 Millionen Euro, aber über den Werten für Japan (3,9 Millionen), Australien (2,6 Millionen) und Großbritannien (2,5 Millionen).[27] Die Firmen

Watch, 2011, S. 20–22; Olaf Böhnke, *Europe's Digital Foreign Policy. Possible Impacts of an EU Online Democracy Promotion Strategy*, Berlin: European Council on Foreign Relations, September 2012.

22 Vgl. Guido Westerwelle, »Die Freiheit im Netz«, in: *Frankfurter Rundschau*, 27.5.2011; »Im Spagat zur Internetfreiheit«, *Deutsche Welle*, 20.6.2013.

23 European Commission, *A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean*, Joint Communication, COM(2011) 200 final, Brüssel, 8.3.2011.

24 Vgl. Solveig Richter/Julia Leininger, *Flexible und unbürokratische Demokratieförderung durch die EU? Der Europäische Demokratiefonds zwischen Wunsch und Wirklichkeit*, Berlin: Stiftung Wissenschaft und Politik, August 2012 (SWP-Aktuell 46/2012).

25 In der deutschen Cybersicherheitsstrategie wird lediglich der Begriff »Cyberangriff« definiert, die Bezeichnung »Cyberkrieg« dagegen vermieden. Vgl. Bundesministerium des Innern, *Cyber-Sicherheitsstrategie* [wie Fn. 2], S. 14. Ein Cyberangriff ist ein IT-Angriff im Cyberraum, der sich gegen ein oder mehrere IT-Systeme richtet, um die IT-Sicherheit zu brechen. Cyberangriffe können die Peripherie von IT-Systemen zum Ziel haben, um deren Verfügbarkeit zu beeinträchtigen (z.B. »Denial of Service«-Angriffe). In diesem Fall werden sie als nicht-intrusive Angriffe bezeichnet. Dringen Cyberangriffe in die Tiefe eines IT-Systems vor (z.B. durch Viren oder Trojaner), um nachhaltig Schaden anzurichten (Abfluss und Zerstörung von Informationen, Fehlfunktionen mit sekundärer Schadwirkung), so handelt es sich um intrusive Angriffe. Die Schadsoftware Flame wurde über Updatemechanismen auf die Rechner gespielt. Immer mehr Staaten, darunter die USA und Großbritannien, setzen inzwischen umfangreiche finanzielle und technische Möglichkeiten ein, um Schwachstellen in IT-Systemen (sogenannte Exploits oder Backdoors in Hard- und Software) zu finden und für eigene Zwecke nutzbar zu machen. Insbesondere sogenannte Zero-Day-Exploits haben Hochkonjunktur. Die Begriffe Cyberspionage oder -ausspähung beziehen sich auf Cyberangriffe, die von fremden Nachrichtendiensten ausgehen oder von diesen gesteuert sind. Cyberausspähung ist ein Cyberangriff, der sich gegen die Vertraulichkeit eines IT-Systems richtet. Der große Teil der Angriffe dient der Informationsabschöpfung. »Cybersabotage« bezeichnet Angriffe gegen die Integrität und Verfügbarkeit eines IT-Systems. Angriffe mit dem Ziel der Sabotage sind sowohl durch extremistische und terroristische Gruppen als auch durch Staaten denkbar. Hochentwickelte Schadsoftware wie Stuxnet steht derzeit nur den USA, Großbritannien, Israel, Russland und China zur Verfügung. Die Schwachstellen der IT-Systeme, die als »Eingangstüren« für diese Angriffe dienen, werden von staatlichen wie nichtstaatlichen Akteuren genutzt. Das macht die eindeutige Zuordnung des Angreifers zu einer der genannten Gruppen schwierig bis unmöglich.

26 Der Begriff Cyberangriff umfasst je nach Urheber und Motiv Formen wie Cybersabotage, Cyberausspähung und Cyberspionage. Gaycken spricht von Cyberrisiken erster, zweiter und dritter Ordnung. Vgl. Sandro Gaycken, »Cybersicherheitsfragen und -antworten«, in: Baums/Scott (Hg.), *Digitale Standortpolitik* [wie Fn. 13], S. 178–182. Rid unterscheidet zwischen Spionage, Sabotage und Subversion, womit der politische Einsatz von Hacking gemeint ist, vgl. »Sabotage durch Hacker ›ist die große Ausnahme‹«, Interview mit Thomas Rid, *dradio.de*, 4.2.2013. Vgl. auch Thomas Rid, *Cyber War Will Not Take Place*, London 2013. Debatten um Cybersicherheit auf beiden Seiten des Atlantiks konzentrieren sich immer stärker auf systemische Risiken. Vgl. Jason Healey (Hg.), *A Fierce Domain: Conflict in Cyberspace. 1986 to 2012*, Vienna, VA, 2013; Christian Pawlik, »Aufbau betriebliches Risikomanagement«, in: *Behörden Spiegel*, November 2012.

27 Ponemon Institute, *2012 Cost of Cyber Crime Study: United States*, Traverse City, MI: Oktober 2012; vgl. auch BDI, *Sicherheit für das Industrieland Deutschland*, Grundsatzpapier, Berlin, Juni 2013, S. 10.

der USA-Stichprobe verzeichnen aktuell 1,8 erfolgreiche Attacken pro Woche. Die Kosten, die US-Unternehmen durch diese Angriffe entstehen, steigen dabei jährlich um rund 40 Prozent. Delikte wie Warenkreditbetrug und Wirtschaftsspionage kommen in den USA ähnlich häufig vor wie in Europa. Das Internet hat zudem neue transatlantische Deliktfelder entstehen lassen. Als größte Herausforderungen für die Kriminalistik gelten Skimming, Phishing, Carding, Schadsoftware, Botnetze, DDoS-Attacken, Account Takeovers und die Underground Economy, die durch die Nutzung von Bitcoins und die in TOR-Netzwerken versteckte Silk Road 2.0 befördert wird. Diese neuen Phänomene entwickeln sich stetig weiter; sie sind flexibel, dynamisch und vor allem anonym.[28]

Das wohl wichtigste Dokument für den transatlantischen Umgang mit Cyberstraftaten ist die sogenannte Cybercrime- oder auch Budapester Konvention.[29] Sie regelt die Zusammenarbeit aller Mitgliedstaaten des Europarates sowie der USA, Kanadas, Japans und Südafrikas.[30] Die Konvention ist der erste internationale Vertrag, der die Harmonisierung nationaler strafrechtlicher Bestimmungen und strafrechtlicher Verfolgung für den Bereich Internet und internetbezogene Straftaten zum Ziel hat. Mit der Konvention wird auf das Problem reagiert, dass die verschiedenen nationalen Bestimmungen strafrechtlich relevanten Handelns außerordentlich heterogen sind und eine Vielzahl von Schlupflöchern aufweisen. Islamisten bauen beispielsweise Online-Foren oftmals in Ländern auf, mit denen kein Rechtshilfeabkommen besteht oder in denen die dort besprochenen Themen keine Straftatbestände darstellen. In geschlossenen Foren werden häufig sogar Anschlagspläne ausgetauscht.[31]

Ein effektiver Rechtsschutz kann jedoch nur schwer gewährleistet werden, wenn nicht einheitlich geregelt ist, was überhaupt strafrechtlich relevant ist und wie mit den Daten mutmaßlicher Straftäter verfahren werden kann. Die 2004 in Kraft getretene Konvention betrifft ein breites Spektrum strafrechtlicher Tatbestände. Sie enthält gemeinsame Kriterien für deren Vorliegen und geeignete Maßnahmen, die staatliche Instanzen gegen solche Rechtsbrüche ergreifen sollen. Hierzu gehören Betrug, Kinderpornographie, Verstoß gegen Rechte geistigen Eigentums und Einbruch in fremde Computersysteme. Mit der Einigung auf die Konvention ist ein großer Schritt in Richtung auf einen gemeinsamen Rechtsraum gelungen.[32]

Ungeachtet ihrer zentralen Rolle für die Verfolgung von Cyberkriminalität hat die Konvention keineswegs zu einer vollständigen Harmonisierung geführt. Ein erster wesentlicher Konfliktpunkt ist die oftmals nur ungenügende Umsetzung der Konvention in nationales Recht. So haben einige EU-Staaten Schwierigkeiten, die europäische Vorratsdatenspeicherung, die auch aus der Budapester Konvention abgeleitet wird, im nationalen Recht zu verankern.[33] Ein weiteres Problem ist das Verbot der Verbreitung rassistischer Propaganda, das in einer Reihe von Staaten (darunter USA, Russland, China, Brasilien und Indien) als Verstoß gegen die freie Meinungsäußerung oder andere nationale Rechtstraditionen verstanden wird.

Die militärische Dimension der Cybersicherheit und das Tallinn Manual

Das sogenannte Tallinn Manual bildet eine wichtige Basis für den transatlantischen Umgang mit militärisch relevanten Cyberbedrohungen. Mit Hilfe des Manuals sollen wesentliche völkerrechtliche Grundlagen den Bedingungen des Cyberzeitalters angepasst werden. Auf Einladung des Cooperative Cyber Defence Centre of Excellence der Nato hat eine Gruppe namhafter Völkerrechtler im estnischen Tallinn insgesamt 95 Richtlinien formuliert, die das Verhalten von Staaten bei Internetangriffen regeln sollen. Die Arbeitsergebnisse erschienen im März 2013.[34] Sie bieten Anknüpfungspunkte für konvergierende und divergierende europäische und US-amerikanische Interpreta-

28 Vgl. Lior Tabansky, »Cybercrime: A National Security Issue?«, in: *Military and Strategic Affairs*, 4 (Dezember 2012) 3, S. 117–136.

29 Europarat, *Übereinkommen über Computerkriminalität*, Budapest, 23.11.2001.

30 Die Tschechische Republik, Griechenland, Irland, Polen und Schweden haben das Abkommen allerdings noch nicht ratifiziert. Nikolaj Nielsen, »EU Seeks US Help to Fight Cyber Criminals«, *EUobserver*, 2.5.2012.

31 Vgl. »Noch viel zu tun. Verfassungsschutz will Cyber-Frühwarnfunktion«, in: *Behörden Spiegel*, März 2013, S. 65.

32 Vgl. Nedife Arslan, »Akkord unbefriedigend«, in: *Adlas – Magazin für Außen- und Sicherheitspolitik*, 7 (2013) 1, S. 26–29.

33 Erich Möchel, »EU plant Vorratsdatenspeicherung 2.0«, *FM4ORF.at*, 22.4.2013, <http://fm4.orf.at/stories/1716492/>; vgl. Jörn Fieseler, »Gesetzentwurf vorlegen! Staatssekretär Klaus-Dieter Fritsche fordert Mindestspeicherfristen«, in: *Behörden Spiegel*, März 2013, S. 63.

34 Michael N. Schmitt (Hg.), *Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence*, Cambridge u.a., 2013.

tionen im Hinblick auf die Definition eines militärischen Angriffs, die Unterscheidung zwischen zivilen und militärischen Zielen und die Bestimmung der Konfliktparteien im Cyberraum. Nato-Vertreter bezeichnen es als »das wichtigste rechtliche Dokument der Cyber-Ära«.[35]

Im Manual wurde festgeschrieben, dass die Bestimmungen der Charta der Vereinten Nationen grundsätzlich auch auf Cyberangriffe anwendbar sind.[36] Der Cyberspace konstituiere weder einen rechtsfreien Raum, noch gälten in ihm völlig andere Rechtsgrundsätze als im physischen Raum. Alle Reaktionen betroffener Staaten oder der internationalen Gemeinschaft müssten daher im Einklang mit den Vorgaben des Völkerrechts stehen.[37] Auch wird in dem Dokument konkretisiert, wann und unter welchen Bedingungen ein kriegerischer Akt vorliegt und mit welchen Maßnahmen Staaten hierauf reagieren dürfen. Regel 13 besagt, dass »[ein] Staat, der im Cyberspace im Ausmaß eines bewaffneten Angriffs attackiert wird«, sich selbst verteidigen darf. Überschreitet eine Cyberaktivität die Schwelle des bewaffneten Angriffs im Sinne des Artikels 51 der VN-Charta, sind Staaten berechtigt, ihr Recht auf Selbstverteidigung wahrzunehmen. Das Manual legt damit den Grundstein dafür, dass Datenattacken mit den Waffen des realen Kriegs beantwortet werden können, wenn sie schwerwiegende Schäden und Todesopfer zur Folge haben.

Allerdings vermeiden die Autoren des Manuals eine klare Festlegung zu den Bedingungen, die ihrer Auffassung nach einen Angriff zu einem kriegerischen Akt werden lassen.[38] Diese Frage, so die Autoren, lasse sich nicht allgemein beantworten, sondern müsse immer im Einzelfall und in Abhängigkeit von ihren Effekten und ihrem Ausmaß beurteilt werden. Dabei ist es von untergeordneter Bedeutung, ob ein Angriff von einem Staat oder einer nichtstaatlichen Gruppe ausgeführt wird. Reine Cyberspionage ist zwar auch nach den Regeln von Tallinn nicht als Kriegshandlung zu betrachten. Spähattacken, die als Vorbereitung eines zerstörerischen Angriffs zu werten sind, könnten allerdings durchaus mit einem präventiven Schlag gegen den Spion beantwortet werden. Staaten hätten zudem auch dann ein Recht auf Verteidigung, wenn der Angreifer eine organisierte Gruppe sei. Das Recht auf Selbstverteidigung gelte hingegen grundsätzlich nicht, wenn eine Einzelperson hinter dem Angriff stehe. Auch Informationslecks begründeten prinzipiell keinen bewaffneten Angriff, wenn sie nicht eine kritische Schwelle überschritten und zu direkten Personenschäden führen könnten.

Die Autoren des Manuals beziehen auch Position zu der Frage, unter welchen Bedingungen eine präventive Selbstverteidigung gegen Cyberangriffe zulässig ist,[39] nämlich dann, wenn ein Angriff »unmittelbar bevorstehe«.[40] Die Crux liegt indes darin, eindeutig zu bestimmen, was unter »unmittelbar« zu verstehen ist. So wird von manchen sogar der Einsatz von Stuxnet »als Akt vorbeugender Selbstverteidigung« gegen das iranische Atomprogramm gesehen.[41] Auch »katastrophale« ökonomische Schäden können nach Auffassung einiger Autoren ein Recht zum Gegenschlag begründen und Selbstverteidigungsmaßnahmen oder Zwangsmaßnahmen des Sicherheitsrates nach Artikel 39 der Charta auslösen. Casus Belli bei den Simulationen der Experten in Tallinn war beispielsweise ein Cyberangriff auf die Wall Street mit mehrtägigem Ausfall der Börse.

Das Tallinn Manual ist nicht unumstritten. Kritiker weisen darauf hin, dass die Definition völkerrechtlicher Regeln für den Cyberkrieg diesen auch »führbarer« macht und dass Normensetzungen zum Umgang mit Angriffen unterhalb der Schwelle des bewaffneten Angriffs bislang fehlen. Bemängelt wird zudem,

35 Thomas Darnstädt/Marcel Rosenbach/Gregor Peter Schmitz, »Cyberwar: Ausweitung der Kampfzone«, in: *Der Spiegel*, (30.3.2013) 14, S. 76–79.
36 Vgl. Harold Hongju Koh, *International Law in Cyberspace*, Washington, D.C.: U.S. Department of State, 18.9.2012, <www.state.gov/s/l/releases/remarks/197924.htm>.
37 Vgl. Interview mit Michael Schmitt, in: »Das Internet ist jetzt Teil des Waffenarsenals«, in: *New Scientist Deutschland*, 19.4.2013, S. 56f. So auch ein ehemaliger Rechtsberater des Internationalen Komitees vom Roten Kreuz: Nils Melzer, »95 Thesen für den korrekten Cyberkrieg«, in: *New Scientist Deutschland*, 28.3.2013, S. 6.
38 Vgl. *Tallinn Manual* [wie Fn. 34], Chapter II: »The Use of Force«, Section 1: »Prohibition of the Use of Force«.
39 Vgl. Ellen Nakashima, »In Cyberwarfare, Rules of Engagement Still Hard to Define«, in: *The Washington Post*, 10.3.2013. Siehe hierzu kritisch: John Arquilla, »Panetta's Wrong about a Cyber ›Pearl Harbor‹«, in: *Foreign Policy*, 19.11.2012.
40 Vgl. *Tallinn Manual* [wie Fn. 34], Chapter II: »The Use of Force«, Section 2: »Self-Defence«.
41 Nach Lewis' Auffassung ist es falsch, die Schadprogramme Stuxnet und Flame als Merkmale einer neuen Art von Kriegsführung darzustellen, auch hätten derartige Angriffe nicht die Zerstörungsgewalt von Nuklearwaffen. James A. Lewis, »In Defense of Stuxnet«, in: *Military and Strategic Affairs*, 4 (2012) 3, S. 65–76. Die Einordnung von Stuxnet als Mittel zur Kriegsführung erschwere internationale Verhandlungen, in denen der Cyberraum verregelt werden soll. Herbert Lin, »Escalation Dynamics and Conflict Termination in Cyberspace«, in: *Strategic Studies Quarterly*, 6 (Herbst 2012) 3, S. 46–70.

dass die Beratungen unter Ausschluss von Experten aus Nicht-Nato-Mitgliedstaaten stattfanden und damit nur eine begrenzte Problemsicht reflektierten.

Gemeinsame transatlantische Initiativen

Die transatlantische Cyberpartnerschaft befindet sich in einem dynamischen Prozess. Hierzu gehören Initiativen im Rahmen der Nato, der EU-USA-Zusammenarbeit, der bilateralen Zusammenarbeit zwischen den USA und einzelnen Mitgliedstaaten sowie vertrauensbildende Maßnahmen gegenüber Dritten.

Aktuelles Grundlagendokument der Nato ist das 2010 veröffentlichte Strategische Konzept. Auch wenn es in diesem Papier nur am Rande um Cybersicherheit geht, wird doch deutlich, dass die Nato das Thema immer mehr für sich entdeckt. »Angriffe auf Computernetze geschehen immer häufiger, sind besser organisiert und kostspieliger, was den Schaden angeht, den sie staatlichen Verwaltungen, Unternehmen, Volkswirtschaften und potenziell auch Transport- und Versorgungsnetzen und anderer kritischer Infrastruktur zufügen.«[42] Derartige Angriffe können dem Konzept zufolge »eine Schwelle erreichen, die den Wohlstand, die Sicherheit und die Stabilität von Staaten und des euro-atlantischen Raums bedroht«,[43] und damit militärische Abwehrmaßnahmen erfordern. Daher sei die Fähigkeit weiterzuentwickeln, »Angriffe auf Computernetze zu verhindern, zu entdecken, sich dagegen zu verteidigen und sich davon zu erholen«,[44] und hierzu sowohl die nötigen staatlichen Kapazitäten aufzubauen als auch die Zusammenarbeit unter den Mitgliedstaaten sowie zwischen ihnen und der Nato zu verbessern. Im Konzept wird nicht ausdrücklich Stellung zu der Frage bezogen, ob Cyberangriffe auch zur Erklärung des Verteidigungsfalls nach Artikel 5 führen und mit dem Beschluss einer kollektiven Verteidigungsreaktion erwidert werden können. Die überwiegende Mehrheit der Staaten scheint diese Frage offen und in Abhängigkeit von der jeweils spezifischen Situation beantworten zu wollen.

Die im Juni 2011 verabschiedete Nato Cyber Defence Policy und der im September 2011 angenommene Aktionsplan konkretisieren das Strategische Konzept für die Cybersicherheitspolitik. Die Nato beginnt eine institutionalisierte Cyberabwehrstruktur aufzubauen, die alle mitgliedstaatlichen Abwehr- und Verteidigungspläne aufeinander abstimmen soll.[45] Auffällig ist hier allerdings, dass sich bisher nur wenige Nato-Mitgliedstaaten dafür stark zu machen scheinen, den Aktionsplan der Nato umzusetzen und Nato-Cyberübungen abzuhalten. Weder Großbritannien noch Frankreich gehören zu dieser Gruppe. Im April 2013 haben die Nato und Russland ihre Absicht verkündet, die Zusammenarbeit in der Cybersicherheit künftig auf die Ebene des Nato-Russland-Rates auszudehnen.[46]

Im November 2010 wurde die EU-USA-Arbeitsgruppe zur Cybersicherheit und Cyberkriminalität gegründet. Sie befasst sich mit dem Problem, dass Cyberangriffe in vielen Fällen entweder gar nicht oder erst nach aufwendigen Ermittlungen (»Forensik«) einem staatlichen oder nichtstaatlichen Akteur zugeordnet werden können. Die erste gemeinsame Planübung von EU und USA im November 2011 (»Cyber Atlantic 2011«) sollte dazu dienen, die Koordinierung zu verbessern und Schwachstellen genauer zu analysieren. Auf Basis der gewonnenen Erkenntnisse veranstaltete die EU ihre zweite europaweite Übung zur Cybersicherheit (»Cyber Europe 2012«), an der mehr als 500 Fachleute aus 29 EU-/EFTA-Staaten teilnahmen. Die Ziele lauteten, kritische Infrastrukturen auf nationaler und europäischer Ebene robuster zu machen und die Zusammenarbeit, Abwehrbereitschaft und Reaktionsfähigkeit im Fall von Cybersicherheitskrisen zu stärken. Die EU und die USA planen für 2014 in ihrer Arbeitsgruppe einen gemeinsamen »Monat der Cybersicherheit«, während dessen die beiderseitigen

42 Nato, *Aktives Engagement, moderne Verteidigung*, Lissabon, 20.11.2010, S. 3.
43 Ebd.
44 Ebd., S. 5.

45 Wichtigstes Gremium im Fall einer Cyberkrise ist das Cyber Defence Management Board (CDMB), das die notwendigen Maßnahmen zur Krisenbewältigung ergreift und über ein Cyber Defence Coordination and Support Center (CD CSC) unter anderem auch die Nato Computer Incident Response Capability (NCIRC) steuert. Die Umsetzung dieser Struktur wird durch das Defence Policy and Planning Committee (DPPC) und das Consultation, Command and Control Board (Nato C3B) überwacht. Im November 2011 fand ein erstes Treffen mit ausgewählten Nato-Partnerstaaten statt (Estland, Spanien, Italien, Deutschland, Lettland, Polen, Ungarn, USA und Niederlande), die auf vergleichbarem technischem Niveau liegen und Interesse an einer Zusammenarbeit bekundet haben. Vgl. »Nato/Defence: Nato Prepares Roadmap for Cyber-Defence«, in: *Europe Diplomacy & Defence*, (26.2.2013) 587; Gerd Lehmann, »Schlüssel zum Erfolg. Kohärentes Führungs- und Aufklärungssystem für NATO und EU«, in: *Behörden Spiegel*, Dezember 2011, S. 54.
46 »Gemeinsam gegen den Cyber-Feind«, in: *Süddeutsche Zeitung*, 24.4.2013, S. 7.

Abwehrmechanismen noch besser aufeinander abgestimmt werden sollen.

Zusammenarbeit bei vertrauensbildenden Maßnahmen

Cyberpolitik hat in vielen Bereichen direkte militärische Relevanz. Damit kein Rüstungswettlauf in der Cyberpolitik in Gang kommt, haben die EU und die USA seit 2011 etliche gemeinsame Initiativen angestoßen, um vertrauens- und sicherheitsbildende Maßnahmen (VSBM) gegenüber Russland und China zu etablieren. Die Debatte über diese Maßnahmen wird insbesondere in den Vereinten Nationen, der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), der G8 sowie bei einer Reihe von Konferenzen geführt (Münchner Sicherheitskonferenz, Londoner Cyberkonferenz mit Folgeveranstaltungen in Budapest und Seoul sowie Berliner Konferenzen). Internationale Organisationen und Foren beschäftigen sich mit Cybersicherheit, darunter die OECD, die ITU Global Cyber Security Agenda, das im Gefolge des Weltinformationsgipfels der VN etablierte Internet Governance Forum und die G20. Hintergrund dieser Gespräche ist eine prinzipiell unterschiedliche Sichtweise über die angemessene Zielsetzung von Regulierungen im Cyberraum. Die Mitgliedstaaten der EU und die USA legen großen Wert auf den freien Zugang zum Cyberraum sowie die Freiheit seiner Inhalte und Nutzung. Dagegen versuchen Russland und China sowie zahlreiche autoritäre Staaten den Cyberraum zu regulieren.[47] In autoritären Staaten bedeutet Cybersicherheit, politisch unerwünschte Inhalte zu unterdrücken und neue Instrumente zu schaffen, um Andersdenkende zu verfolgen. Die Entwicklung und Umsetzung vertrauensbildender Maßnahmen sieht sich daher mit oftmals diametral entgegengesetzten Zielen regulativen Handelns konfrontiert. Für die EU und die USA bleiben der Zugang zum Cyberraum sowie die Freiheit seiner Inhalte und seine Nutzung unter Beachtung rechtsstaatlicher und demokratischer Prinzipien ein entscheidender Aspekt, der bei Sicherheitsmaßnahmen berücksichtigt werden muss. Diese beziehen sich insbesondere auf verantwortbares staatliches Handeln im Cyberraum sowie auf das Spannungsverhältnis zwischen Sicherheit des Cyberraums und Informationsfreiheit.

Multilaterale völkerrechtliche Verträge nach dem Muster der Abrüstung und Rüstungskontrolle sind derzeit nicht durchsetzbar, weil zwischen den USA und Europa auf der einen und Russland und China auf der anderen Seite elementare Differenzen über die Nutzung des Cyberraums für militärische Operationen bestehen.[48] Bei vielen Fragen sind die Gräben augenblicklich kaum zu überwinden, so bei der Implementierung und Verifikation, der Definition von Cyberwaffen sowie der völkerrechtlichen beziehungsweise strafrechtlichen Zurechnung (Attribution) von Angriffen. Die Mitgliedstaaten der EU setzen sich daher in enger Abstimmung mit den USA, Kanada, Japan und Australien in den VN und der OSZE dafür ein, einen Verhaltenskodex für staatliche Aktivität im Cyberraum zu entwickeln.[49] Die mit einem Mandat der VN-Vollversammlung ausgestattete Gruppe aus insgesamt 15 Regierungsvertretern hat der 68. Vollversammlung im Juni 2013 ihren Abschlussbericht zu verantwortlichem Staatenhandeln im Cyberraum vorgelegt sowie Vorschläge zu vertrauensbildenden Maßnahmen unterbreitet.[50] Wegen der tiefgreifenden Meinungsverschiedenheiten zwischen demokratischen und autoritären Staaten haben bilaterale Cyberdialoge Hochkonjunktur.[51] Die USA und Deutschland haben speziell mit Russland Übereinkünfte getroffen und mit China Dialoge eingerichtet. Dabei geht es um Schwerpunkte der jeweiligen Gefährdungseinschätzung sowie die jeweilige Position der in der VN GGE (Group of Governmental Experts der Vereinten Nationen) zu verhandelnden Normen für staatliches Verhalten im Cyberraum.[52] Auch hier offenbaren sich

47 Eine übersichtliche und differenzierte Gesamtschau von Positionen zur Normenentwicklung im Cyberspace bietet die Website *citizenlab.org*. Für die US-Perspektive vgl. Richard A. Clarke/Robert K. Knake, *Cyber War*, New York 2010, Kapitel 7.

48 Vgl. James A. Lewis, »Multilateral Agreements to Constrain Cyberconflict«, in: *Arms Control Today*, 40 (Juni 2010) 5, S. 14–19.

49 Die Konferenz der OSZE zur Cybersicherheit im Mai 2011 zeigte, dass zahlreiche Staaten die OSZE mit ihren Erfahrungen in blockübergreifender Rüstungskontrolle und Vertrauensbildung als geeigneten Rahmen sehen, vertrauens- und sicherheitsbildende Maßnahmen auch für den Cyberraum zu entwickeln. Vgl. Tim Maurer, *Cyber Norm Emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security*, Cambridge, MA: Belfer Center for Science and International Affairs, September 2011.

50 Neben den USA ist auch Deutschland in der VN-Regierungsexpertengruppe zu Cybersicherheit vertreten.

51 »Russia, U.S. Will Try to Reach Agreements on Rules Governing Information Security – Newspaper«, *Interfax*, 29.4.2013; »US, China Discuss Cyber Security as Dialogue Begins«, *Voice of America*, 9.7.2013.

52 Jane Perlez, »U.S. and China Put Focus on Cybersecurity«, in: *The New York Times*, 22.4.2013.

allerdings sehr schnell wieder gravierende Differenzen. Russland möchte den Einsatz von Cyberwaffen generell ächten,[53] die USA lehnen dies ab. Experten sehen die wichtigsten Gründe dafür in der technischen Überlegenheit der USA und der Schwierigkeit, die Einhaltung derart weitreichender Abkommen verlässlich zu überwachen.[54]

53 Rex Hughes, »A Treaty for Cyberspace«, in: *International Affairs*, 86 (2010) 2, S. 523–541.
54 *Draft Convention on International Information Security*, Jekaterinburg, September 2011.

Konfliktthemen

Trotz der offensichtlich großen Gemeinsamkeiten zwischen den USA und den Mitgliedstaaten der EU gibt es in den transatlantischen Cyberbeziehungen auch eine ganze Reihe erheblicher Dissonanzen. Sie betreffen den angestrebten globalen Regelungsmodus des Internet (globale Konflikte), die sehr unterschiedlichen Sicherheitskonzeptionen auf beiden Seiten des Atlantiks (transatlantische Konflikte) und die transnationalen Beziehungen (transnationale Konflikte). Zudem hat Großbritannien starke Vorbehalte im Hinblick auf Europas gemeinschaftliche Vorgehensweise in der Innen- und Justizpolitik. Die besondere Rolle des Landes in der europäischen Innen- und Justizpolitik und ihre Auswirkungen auf die transatlantische Zusammenarbeit werden im Folgenden jedoch nicht näher ausgeführt.

Globale Konflikte

Öffnung des Multistakeholder-Ansatzes

Ein erster wichtiger Konfliktpunkt ist das überkommene Multistakeholder-Modell zur Regulierung des Internet. Mehrere Schwellenländer mit beachtlichem Wirtschaftswachstum, wie Brasilien, Indien, Südafrika, die Türkei und Indonesien, fühlen sich in Gremien wie ICANN und IGF nur ungenügend berücksichtigt und verlangen, dass intergouvernementale Gremien wie die ITU eine größere Rolle spielen. Bis heute beschränkte sich die ITU auf die Standardisierung und den Aufbau technischer Kapazitäten in Entwicklungsländern. Ihre Arbeit bestand wesentlich in der Verwaltung des Vertrags über die International Telecommunication Regulations (ITR), mit dem die Interoperabilität des internationalen Telefonsystems gewährleistet wird. Bei der World Conference on International Telecommunication (WCIT) im Dezember 2012 in Dubai eskalierte der Streit zwischen den USA, Europa und einigen anderen westlichen Staaten auf der einen und den IBSA/BRIC-Staaten auf der anderen Seite. Letztere forderten, den ITR-Vertrag neu auszuhandeln, mit der Absicht, seine Reichweite auf das Internet auszudehnen und die Kompetenzen der intergouvernementalen ITU deutlich auszuweiten.[55] Im Hintergrund dieser Forderung stand das Ziel, die Hegemonie der USA in der Verwaltung des Internet zu brechen und eine neue Ordnung zu schaffen, in der die Staaten des Südens mehr Gewicht haben würden.

Bei den USA, Europa, Japan, Australien und Kanada stießen diese Forderungen allerdings auf wenig Gegenliebe. Die westlichen Staaten lehnten es ab, das Multistakeholder-Modell grundsätzlich in Frage zu stellen und die ITU mit neuen Befugnissen auszustatten. Sie wiesen sogar den vorsichtigen Kompromissvorschlag zurück, den ITR zumindest um allgemeine Erklärungen zur »Zusammenarbeit der Regierungen zu Spam« und zur »Netzwerksicherheit« sowie einer rechtlich nicht verbindlichen Zusatzerklärung zur Arbeit der ITU im Bereich Internet-Regulierung[56] zu erweitern.

Aufgrund der Snowden-Enthüllungen vom Sommer 2013 scheint die Abwehrfront der westlichen Staaten gegen Forderungen nach einer Neuorganisation der Internet Governance erstmals zu bröckeln.[57] Die EU befürwortet zwar nach wie vor einen Multistakeholder-Ansatz, drängt aber energischer darauf, demokratische Staaten wie Brasilien und Indien mehr einzubinden. EU-Kommissarin Neelie Kroes verlangte jüngst, inklusive und transparente Verfahren zu gewährleisten.[58] Die bisherige Praxis einseitiger Dominanz der USA und ihrer Verbündeten in Gremien wie ICANN müsse korrigiert werden. Im Gegensatz zu den USA spricht sich die EU dafür aus, das Governmental Advisory Committee (GAC) innerhalb von ICANN zu stärken und damit das intergouvernementale Prinzip zu betonen. Die Europäische Kommission hat zudem

55 Ben Scott/Tim Maurer, »Digitale Entwicklungspolitik«, in: Baums/Scott (Hg.), *Digitale Standortpolitik* [wie Fn. 13], S. 126f; Hannes Ebert/Tim Maurer, »Contested Cyberspace and Rising Powers«, in: *Third World Quarterly*, 34 (2013) 6, S. 1054–1074.
56 Vgl. Tim Maurer, *What Is at Stake at WCIT? An Overview of WCIT and the ITU's Role in Internet Governance*, Washington, D.C.: New America Foundation, Open Technology Institute, 5.12.2012; Isabel Skierka, »Kampf um die Netzherrschaft«, in: *Adlas – Magazin für Außen- und Sicherheitspolitik*, 7 (2013) 1, S. 12–16.
57 »Internet Governance Forum der UN: Netzpolitik im Zeitalter von NSA-Netzüberwachung«, *heise.de*, 21.10.2013.
58 Neelie Kroes, *Building a Connected Continent*, Brüssel: European Commission, SPEECH/13/741, 24.9.2013.

im Juni 2013 vorgeschlagen, ein Global Internet Policy Observatory zu gründen. In Zusammenarbeit mit Brasilien, der Afrikanischen Union, der Schweiz und einigen nichtstaatlichen Verbänden soll es für mehr Transparenz und faktische Teilhabechancen in der Internet Governance sorgen.

Brasilien und Deutschland wollen den Internationalen Pakt über bürgerliche und politische Rechte ergänzen und erweitern, der von den VN 1966 beschlossen wurde und 1976 in Kraft trat.[59] Dieser sogenannte Zivilpakt soll für die digitalisierte Welt fortgeschrieben werden. Eine überwältigende Mehrheit der 193 VN-Mitgliedstaaten unterstützt diese Initiative. Unabhängig davon, wie diese verschiedenen Vorstöße im Einzelnen zu bewerten sind und ob sie eine nachhaltige Änderung der bestehenden Governancestruktur des Internet versprechen – es dürfte offensichtlich sein, dass die EU, aber auch andere Staaten wie Brasilien, Indien, Türkei oder Indonesien den Druck auf die USA erhöhen werden und dass die Forderungen nach einer partizipativeren Ordnung nicht länger beiseitegeschoben werden können.[60]

Technologische Souveränität

Snowdens Enthüllungen haben nicht nur dafür gesorgt, dass der Ruf nach einer neuen Organisation für die Regulierung des Internet immer lauter wurde. Sie haben auch neue Bemühungen um eine bessere nationale Kontrolle von Kommunikationsinfrastrukturen angestoßen. Die Europäische Kommission hat hierzu Ende September 2012 eine Strategie zur »Freisetzung des Cloud-Computing-Potentials in Europa«[61] vorgelegt. Während diese ursprünglich vor allem ökonomisch motiviert war und Arbeitsplätze schaffen sollte, hat die Aufdeckung US-amerikanischer Überwachungspraktiken bewirkt, dass sich das Motiv der »Datensouveränität« (data sovereignty) in den Vordergrund geschoben hat. Die Strategie sieht vor, dass die technischen Normen der Mitgliedstaaten weiter harmonisiert werden. Zudem sollen EU-weite Zertifizierungsprogramme für vertrauenswürdige Cloud-Anbieter unterstützt sowie sichere und faire Mustervertragsbedingungen erarbeitet werden. Die Kommission will eine Europäische Cloud-Partnerschaft mit den Mitgliedstaaten und der Branche etablieren, um die Marktmacht des öffentlichen Sektors besser nutzen zu können. Hierdurch sollen europäischen Cloud-Anbietern größere Chancen eröffnet werden, eine wettbewerbsfähige Größe zu erreichen und sich gegen US-amerikanische Konkurrenten zu behaupten.

Nach Auffassung der Europäischen Kommission muss auch ein EU-weites Cloud-Computing-System entwickelt werden, um europäischen Verwaltungen und privaten Firmen die nötige Sicherheit vor Spionage zu geben. Dateien, die auf Cloud-Plattformen wie Dropbox, Google Drive oder Skydrive abgelegt werden, können sich als ernstes Sicherheitsrisiko herausstellen. Gefahren lauern beispielsweise in Servern außerhalb Europas und in Allgemeinen Geschäftsbedingungen, die teilweise weitreichende Zugriffsrechte auf den Inhalt einschließen. Nicht auszuschließen sind auch Einbruchsszenarien wie zuletzt bei Dropbox. US-Behörden können sich heimlich Zugriff auf die Daten europäischer Nutzer bei Cloud-Anbietern wie Google, Facebook oder Dropbox verschaffen.

Auch eine vom EP-Ausschuss für bürgerliche Freiheiten, Justiz und Inneres 2012 in Auftrag gegebene Studie zeigt, dass Cloud Computing vor allem dann ein relevantes Sicherheitsrisiko darstellt, wenn Daten auf den Servern von US-Anbietern liegen.[62] Juristen der Universität Amsterdam haben im November 2012 darauf hingewiesen, dass der Patriot Act US-Geheimdiensten umfangreiche Zugriffsrechte auf Kommunikations- und Nutzerdaten einräumt.[63] Auf Grundlage der amerikanischen Antiterrorgesetze Patriot Act und Foreign Intelligence Surveillance Amendments Act (FISAA) von 2008, der bis 2017 verlängert wurde,

59 Der Pakt (International Covenant on Civil and Political Rights, ICCPR) untersagt »willkürliche oder illegale Eingriffe in die Privatsphäre, die Familie, die Wohnstätte oder den Briefverkehr« sowie »ungesetzliche Angriffe auf Ehre und Ansehen«. Er gehört neben der Allgemeinen Erklärung der Menschenrechte von 1948 zu den grundlegenden Rechtstexten der VN zu den Menschen- und Bürgerrechten.

60 Vgl. Internet Governance Project (IGP), *Comments of the Internet Governance Project on the ICANN Transition*, Juni 2009; IGP, *The Core Internet Institutions Abandon the US Government*, 11.10.2013; Monika Ermert, »›Nicht irgendein Internet‹: Brasilien fordert auf UN-IGF Konsequenzen aus der NSA-Affäre«, *heise.de*, 22.10.2013.

61 European Commission, *Unleashing the Potential of Cloud Computing in Europe*, COM(2012) 529 final, Brüssel, 27.9.2012.

62 Didier Bigo et al., *Fighting Cyber Crime and Protecting Privacy in the Cloud*, Brüssel: EP, Oktober 2012; Didier Bigo et al., *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law*, Brüssel: EP, Oktober 2013.

63 J. V. J. van Hoboken et al., *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act*, Amsterdam: Institute for Information Law, November 2012.

können US-Ermittler bei Gericht einen geheimen Beschluss beantragen und ausländische Nutzer überwachen. Demnach müssen nicht nur amerikanische Cloud-Anbieter wie Google oder Amazon die Daten ihrer Kunden auf Anfrage (optional mit der Verpflichtung zur Geheimhaltung) herausgeben – ungeachtet dessen, ob diese Daten auf Servern in Europa oder den USA gespeichert sind. Es können auch europäische Firmen betroffen sein, die in den USA geschäftlich tätig sind. Die Autoren der EP-Studie empfehlen, der Rechtssicherheit beim Cloud Computing Vorrang zu gewähren. Ziel der EU solle es deshalb sein, bis zum Jahr 2020 wenigstens 50 Prozent der EU-Dienste auf Cloud-Computern unter eigene rechtliche Kontrolle zu stellen.[64]

In Deutschland ist die Idee der technologischen Souveränität schon seit einigen Jahren bekannt. Im Juni 2010 warb Bundesinnenminister Thomas de Maizière dafür, die technologische Souveränität zu wahren.[65] Die Bundesregierung hat im Juli 2013 einen Acht-Punkte-Plan vorgelegt, der detaillierte erste Maßnahmen enthält, um die US-amerikanischen Spionagetätigkeiten zu beantworten. Dieses Maßnahmenbündel soll helfen, neue Sicherheitsstandards und den Zugang zu Risikokapital zu erleichtern. Auf europäischer Ebene soll eine ehrgeizige IT-Strategie vorangetrieben werden, um Anbieter internetgestützter Geschäftsmodelle mit hoher Sensibilität für die Sicherheit der Internetnutzer zu fördern. Neue Startups sollen motiviert und finanziell unterstützt werden. Die Debatte über die technologiepolitischen Implikationen der NSA-Praktiken mündete in die von der Deutschen Telekom lancierte Idee des »Schengen Routing«.

Bei diesen Entwicklungen handelt es sich um weit mehr als um bloße staatliche Wirtschaftsförderungspolitik. Hier findet ein globaler Paradigmenwechsel statt: Das Vertrauen ins freie Spiel der Marktkräfte ist verlorengegangen, und als entscheidendes Kriterium für die Sicherheit der angebotenen IT-Systeme gilt nunmehr der physische Ort des Firmensitzes. Es geht um die Frage der »Vertrauenswürdigkeit«, und »fremden« Unternehmen wird grundsätzlich mit Misstrauen begegnet. Nicht ganz zu Unrecht wird auf das Übergewicht amerikanischer Internetfirmen und die Tatsache hingewiesen, dass wichtige IT-Geräte in Asien hergestellt werden. Im Gegenzug sollen »eigene« Technologien entwickelt und produziert werden. Nicht mehr das Zusammenwachsen der Märkte, sondern der Aufbau nationaler Autarkie droht zum Maßstab politischen Handelns zu werden.

Transatlantische Konflikte

Die Cybersicherheitspolitik der USA und der EU ist von zwei sehr unterschiedlichen Grundideen geprägt. Während in den USA die militärische Abschreckung dominiert, soll Sicherheit aus europäischer Perspektive vor allem mit polizeilichen Maßnahmen und einer verbesserten Widerstandsfähigkeit (resilience) gegen Angriffe gewährleistet werden.

Die US-Strategie – Auf dem Weg zur digitalen Abschreckung

Die Cyberverteidigung ist von zentraler Bedeutung für die USA. Zuständig hierfür ist das 2010 gegründete US Cyber Command des Pentagon, das rund 900 Mitarbeiter hat und dem US Strategic Command (USSTRATCOM) zugeordnet ist. Es sitzt in Fort Meade in unmittelbarer Nähe der National Security Agency (NSA), des größten Geheimdienstes der Vereinigten Staaten.[66] Der Auftrag des US Cyber Command besteht darin, Verteidigungsmaßnahmen gegen mögliche Angriffe zu organisieren (Computer Network Defense) und gleichzeitig eine offensive Angriffsfähigkeit aufzubauen (Cyber Attack Operations). Wie wichtig diese Maßnahmen aus Sicht der USA sind, lässt sich daran ablesen, dass die Mitarbeiterzahl des Cyber Command künftig auf rund 4900 Mitarbeiter aufgestockt, also mehr als verfünffacht werden soll. Es sollen 13 Cyberangriffsteams gebildet werden, die sogenannte Cyber-Kinetic Attacks ausführen können, also Cyberangriffe, die Objekte zerstören.[67]

Die herausragende Bedeutung der Sicherheitsagenda schlägt sich auch in den eingesetzten finanziellen Mitteln nieder. Das Pentagon hat für das Jahr 2014 4,7 Milliarden US-Dollar beantragt, etwa eine Milliarde mehr als der Vorjahresetat. In den nächsten vier Jahren sollen weitere 23 Milliarden Dollar investiert

64 Bigo et al., *Fighting Cyber Crime* [wie Fn. 62], S. 50.
65 Vgl. Thomas de Maizière, *14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft*, Berlin: Bundesministerium des Innern, 22.6.2010.
66 Zur Entwicklung der US-Geheimdienstpolitik siehe James Bamford, *The Shadow Factory. The Ultra-secret NSA from 9/11 to the Eavesdropping on America*, New York u.a., 2008.
67 Vgl. »Pentagon Reviews ›Rules of Engagement‹ against Cyber Attacks«, in: *Europe Diplomacy & Defence*, (4.7.2013) 620.

werden.[68] Die 16 Geheimdienstbehörden der USA beschäftigen insgesamt über 107 000 Mitarbeiter. Für die Arbeit der Geheimdienste hat die US-Regierung im Haushaltsjahr 2013 52,6 Milliarden Dollar veranschlagt.[69] Die größte Summe beantragte die Central Intelligence Agency (CIA) mit 14,7 Milliarden Dollar. An zweiter Stelle steht die auf das Ausspionieren elektronischer Kommunikation spezialisierte NSA, deren Budget 10,8 Milliarden Dollar umfasst. In etwa 80 US-Botschaften und Konsulaten gibt es nach Berichten des Nachrichtenmagazins *Der Spiegel* geheime Lauschposten, die intern Special Collection Service (SCS) genannt und gemeinsam mit der CIA betrieben werden. Die kleinen SCS-Teams fangen aus vielen diplomatischen Vertretungen heraus die Kommunikation in ihren jeweiligen Gastländern ab. Diese Art technischer Aufklärung läuft NSA-intern unter dem Codenamen »Stateroom«. Das National Reconnaissance Office (NRO) schließlich, das für die Spionagesatelliten verantwortlich ist, erhielt im Haushaltsjahr 2013 10,3 Milliarden Dollar.

Die Cybersicherheitspolitik der USA ist wesentlich von der Vorstellung geprägt, dass die nationale Sicherheit bedroht sei und dieser Bedrohung mit militärischem Denken und militärischen Mitteln begegnet werden müsse. Schon zwei Jahre nach den Anschlägen vom 11. September 2001 veröffentlichte das Weiße Haus seine National Strategy to Secure Cyberspace.[70] Darin wurde die amerikanische Cybersicherheitspolitik noch in den Terrorismuskontext gestellt und überwiegend auf die Bedrohung durch nichtstaatliche Akteure zugeschnitten.[71] Im Laufe der nächsten Jahre relativierte sich diese Sichtweise jedoch zusehends und wurde durch eine Analyse der von China und Russland ausgehenden Bedrohung erweitert.

Abschreckung und die Drohung mit massiven Reaktionen sind heute Kernelemente der US-Cybersicherheitspolitik.[72] Im Mai 2011 präsentierten die Vereinigten Staaten ihre International Strategy for Cyberspace, in der sie keinen Zweifel daran lassen, dass sie jeden feindlichen Akt im Cyberspace mit entsprechenden Gegenmaßnahmen beantworten werden: »When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.«[73] Nur zwei Monate später kündigte das US-Verteidigungsministerium an, jeder Angriff auf kritische Infrastrukturen in den USA werde einen Vergeltungsschlag zur Folge haben.[74] Der damalige US-Verteidigungsminister Leon Panetta warnte, den USA drohe ein »Cyber Pearl Harbor«, wenn sie ihre Verteidigung nicht stark ausbauten.[75] »Wir müssen unseren Feinden wirklich Angst einjagen«, so auch der ehemalige General James Cartwright, Autor der gültigen Cyberstrategie des Pentagons.[76]

Abschreckung gegenüber Angriffen aus dem Cyberspace ist in Literatur und Politik gleichwohl sehr umstritten. Viele Experten argumentieren, dass sich Angriffe oftmals überhaupt nicht eindeutig zuordnen lassen und Abschreckung deswegen ins Leere ginge. Auch die US-Regierung geht offiziell davon aus, dass sie lediglich ein Drittel der Angriffe zweifelsfrei einem bestimmten Urheber zuschreiben könne.[77] Im Mandiant-Bericht dagegen heißt es, US-Geheimdienste und -Militär wüssten weit mehr über die heimlichen Aktivitäten potentieller Angreifer, als sie öffentlich

68 James Bamford, »The Secret War. Infiltration. Sabotage. Mayhem. For Years, Four Star General Keith Alexander Has Been Building A Secret Army Capable of Launching Devastating Cyberattacks«, *Wired*, 12.6.2013.

69 Die Enthüllungen des Informanten Edward Snowden geben einen Einblick in den streng vertraulichen Haushalt der US-Geheimdienste. Die *Washington Post* veröffentlichte auf ihrer Internetseite Auszüge des unter Verschluss gehaltenen »Black Budget« der US-Regierung. Barton Gellman/Greg Miller, »U.S. Spy Network's Successes, Failures and Objectives Detailed in ›Black Budget‹ Summary«, in: *The Washington Post*, 29.8.2013, <www.washingtonpost.com/wp-srv/special/national/black-budget/>.

70 Vgl. Neil Robinson et al., *Cyber-security Threat Characterisation. A Rapid Comparative Analysis*, Cambridge: RAND Europe, 2013, S. 28–32.

71 Nye sieht eher die Möglichkeit eines »Cyber 9/11«: Joseph S. Nye, »What Is It That We Really Know about Cyber Conflict?«, in: *The Daily Star*, 24.4.2012.

72 Center for Strategic and International Studies (CSIS), *Cybersecurity Two Years Later. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Washington, D.C., Januar 2011.

73 The White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, Washington, D.C., Mai 2011.

74 Eine kritische Auseinandersetzung mit der Strategie liefert Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, September 2013.

75 Elisabeth Bumiller/Thom Shanker, »Panetta Warns of Dire Threat of Cyberattack on U.S.«, in: *The New York Times*, 11.10.2012.

76 Zitiert nach Darnstädt/Rosenbach/Schmitz, »Cyberwar« [wie Fn. 35].

77 Zitiert nach »Sicherheitsexperte Lewis über Cyber-Krieg: ›Wir müssen unsere Verteidigung stärken‹« (Interview mit James Lewis), in: *Süddeutsche Zeitung*, 2.2.2012, S. 16.

zugäben.[78] Die U.S.-China Economic and Security Review Commission wiederum verlangt in ihrem Bericht von November 2013 an den Kongress, Amerika müsse umfassend auf die chinesische Spionage im Internet reagieren. Sie erwägt Handelsbeschränkungen, Einreiseverbote für Organisationen mit Hackerkontakten und eine Bankensperre für Firmen, die im Internet gestohlenes geistiges Eigentum verwenden. Bestehende Sanktionen könnten noch verschärft werden.[79] Der Grundgedanke der Abschreckung solle demnach auch im digitalen Zeitalter funktionieren.[80] Erste Vorschläge für eine Cyber-Abschreckungsstrategie[81] beinhalten den Ausbau der eigenen militärischen Stärke, die Fähigkeit, einen Erstschlag auszuführen, und die Möglichkeit, einem Cyberangriff nahezu in Echtzeit militärisch begegnen zu können.[82] Hierzu müsse die technologische und wissenschaftliche Führungsposition der USA bewahrt werden. Ziele und Motive potentieller Angreifer müssten schnell identifiziert und angemessene Gegenmaßnahmen ergriffen werden können. Die keineswegs nur defensive Ausrichtung der amerikanischen Cybersicherheitsmaßnahmen wird darin deutlich, dass die US-Geheimdienste 2011 alleine 231 offensive Cyberoperationen starteten. Hierfür wurden 652 Millionen US-Dollar unter dem Programm GENIE bereitgestellt und insgesamt 1870 Computerspezialisten beschäftigt, um in ausländische Netzwerke einzudringen.[83]

78 Im Februar 2013 veröffentlichte die private US-Sicherheitsfirma Mandiant einen Bericht über die Verwicklung von Einheiten des chinesischen Militärs in massive Cyberspionage. *APT1: Exposing One of China's Cyber Espionage Units*, Alexandria, VA: Mandiant, 2013.

79 Die Kommission begründet ihre harte Gangart damit, dass China keine Reue zeige, und beruft sich dabei auf die bereits genannte Firma Mandiant. Diese hatte im Februar 2013 zum ersten Mal eine konkrete Einheit der Volksbefreiungsarmee als Ausgangspunkt von Hackerangriffen gegen westliche Wirtschaftsunternehmen identifiziert. Mandiant berichtete im November 2013, die Einheit habe nach ihrer Enttarnung einen Monat Pause gemacht und danach ihre Aktionen mit neuer Schadsoftware einfach fortgesetzt. U.S.-China Economic and Security Review Commission, *2013 Annual Report to Congress*, Washington, D.C., 20.11.2013, <www.uscc.gov/Annual_Reports/2013-annual-report-congress>.

80 Vgl. Tim Stevens, »A Cyberwar of Ideas? Deterrence and Norms in Cyberspace«, in: *Contemporary Security Policy*, 33 (2012) 1, S. 148–170; Paul-Anton Krüger, »Digitale Abschreckung. Die USA sind bereit, Cyberangriffe mit aller Härte zu beantworten«, in: *Süddeutsche Zeitung*, 21.2.2013, S. 4.

81 Für Cyberabschreckung plädiert Joseph S. Nye, *The Future of Power*, New York 2011, Kapitel 5. Eine kritische Sichtweise auf die Idee der »deterrence« bietet Stevens, »A Cyberwar of Ideas?« [wie Fn. 80].

82 Vgl. Frank J. Cilluffo/Sharon L. Cardash/George C. Salmoiraghi, »A Blueprint for Cyber Deterrence: Building Stability through Strength«, in: *Military and Strategic Affairs*, 4 (2012) 3, S. 3–23.

83 Nye, *The Future of Power* [wie Fn. 81].

EU-Strategie zur Cybersicherheit: Resilience und Kriminalitätsbekämpfung

Die europäische Strategie zur Cybersicherheit unterscheidet sich grundlegend von der Strategie der USA. Nicht Abschreckung, sondern der Aufbau von Widerstandsfähigkeit (resilience) und die Bekämpfung von Kriminalität bilden die Schwerpunkte europäischen Handelns. Die EU-Politik hat vier wesentliche Komponenten. Sie basiert auf einer 2013 von der Europäischen Kommission und dem Europäischen Auswärtigen Dienst präsentierten Cybersicherheitsstrategie, einem Richtlinienvorschlag für Netz- und Informationssicherheit (NIS), einem neu gegründeten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (European Cybercrime Centre, EC3) sowie einer Reihe spezifischerer Projekte zur Widerstandsfähigkeit.

Die europäische Cybersicherheitsstrategie[84] wurde Ende Juni 2013 verabschiedet. Sie soll die Sicherheit von Informationstechnologien sowie die Einhaltung der Grundrechte und Grundwerte der EU gewährleisten. Der Ausbau militärischer und geheimdienstlicher Fähigkeiten nimmt in der Strategie vergleichsweise wenig Raum ein. Von den fünf dort genannten Schwerpunkten des EU-Handelns bezieht sich nur einer auf die Entwicklung einer Cyberverteidigungspolitik. Die vier anderen betreffen den Aufbau verbesserter nichtmilitärischer Kapazitäten. Im Einzelnen geht es um Widerstandsfähigkeit gegenüber Cyberangriffen, Eindämmung der Cyberkriminalität, Ausbau industrieller und technischer Ressourcen für die Cybersicherheit und Formulierung einer einheitlichen Cyberraumstrategie.[85]

84 Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik, *Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, Brüssel*, JOIN(2013) 1 final, Brüssel, 7.2.2013.

85 Vgl. Patryk Pawlak, *Cyber World: Site under Construction*, Paris: European Union Institute for Security Studies (EUISS), September 2013. Grundlegend zur europäischen Cybersicherheitspolitik: Annegret Bendiek, *Europäische Cybersicherheitspolitik*, Berlin: Stiftung Wissenschaft und Politik, Juli 2012 (SWP-Studie 15/2012).

In dem begleitenden, derzeit noch nicht verabschiedeten Richtlinienvorschlag für Netz- und Informationssicherheit (NIS) hebt die Europäische Kommission die besondere Rolle privatwirtschaftlicher Unternehmen hervor. Nicht nur die Mitgliedstaaten, sondern auch die Betreiber kritischer Infrastrukturen müssten demnach zum Schutz der weltweiten digitalen Infrastruktur beitragen. Die Unternehmen sollen dafür sorgen, dass ihre Produkte und Dienstleistungen stets aktuellen Sicherheitsstandards genügen und so gut wie möglich gegen Angriffe gewappnet sind.[86] Die Kosten der Einrichtung einer sicheren Infrastruktur für den Informationsaustausch zwischen den Mitgliedstaaten werden auf 10 Millionen Euro jährlich geschätzt. Ende Juni 2013 hat die EU eine Verordnung für Kommunikationsunternehmen erlassen. Danach sind Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste verpflichtet, »unverzüglich die zuständige nationale Behörde und in bestimmten Fällen auch die von Verletzungen des Schutzes personenbezogener Daten betroffenen Teilnehmer und Personen zu benachrichtigen«.[87]

Institutionell findet die Cyberkriminalitätsbekämpfung der EU ihren Niederschlag im Ausbau des neu geschaffenen Europäischen Zentrums zur Bekämpfung der Cyberkriminalität (EC3). Es wird Analysen und Informationen liefern, Untersuchungen unterstützen, forensische Arbeiten ausführen, die Zusammenarbeit unter den Mitgliedstaaten erleichtern, dem Privatsektor und anderen Akteuren Informationen zur Verfügung stellen und langfristig als Sprachrohr der Strafverfolgungsbehörden insgesamt fungieren.

Weitere Maßnahmen der EU beinhalten ein Anfang 2013 begonnenes und mit 15 Millionen Euro ausgestattetes Pilotprojekt zur Bekämpfung von Botnets und Schadprogrammen sowie die finanzielle Unterstützung wichtiger Infrastrukturen, die die NIS-Kapazitäten der Mitgliedstaaten miteinander verknüpfen (Fazilität »Connecting Europe«). Ziel ist der umfassende Schutz von Vermögenswerten und Personen, insbesondere durch öffentlich-private Partnerschaften wie die European Public-Private Partnership for Resilience (EP3R) und Trust in Digital Life (TDL). Die Arbeiten sollen sich auf die Sicherheit der Lieferkette konzentrieren. Einbeziehen sollen sie dabei die laufenden Normungsarbeiten der europäischen Normenorganisationen (Comité Européen de Normalisation, CEN; Comité Européen de Coordination des Normes Électriques, CENELEC; European Telecommunications Standards Institute, ETSI) und der Koordinierungsgruppe für die Cybersicherheit (Cyber Security Coordination Group, CSCG) sowie die Fachkenntnis der European Network and Information Security Agency (ENISA), der Europäischen Kommission und anderer relevanter Akteure. Mit dem Rahmenprogramm »Horizont 2020« für Forschung und Innovation soll zusätzlich die Entwicklung von Instrumenten zur Bekämpfung krimineller und terroristischer Aktivitäten im Cyberraum finanziert werden. Es wird Arbeiten zur Sicherheitsforschung mit neuer Informations- und Kommunikationstechnologie unterstützen. Der neue mehrjährige Finanzrahmen der EU für die Periode 2014 bis 2020 umfasst rund 80 Milliarden Euro für »Horizont 2020«, das bislang größte Forschungsprogramm der EU. Über 1,5 Milliarden Euro entfallen auf die Sicherheitsforschung. 400 Millionen Euro davon werden für Forschungen zur Cybersicherheit bereitgestellt.

Schutz kritischer Infrastrukturen

Das US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) berichtete im Juli 2012, dass die Zahl der Cyberangriffe auf kritische Infrastrukturen der USA binnen zwei Jahren von 9 (2009) auf 198 (2011) gestiegen ist.[88] Die ENISA hat ihren ersten Bericht im Januar 2013 veröffentlicht und ebenfalls auf die wachsenden Cyberrisiken für die kritische

86 Annegret Bendiek, *Kritische Infrastrukturen, Cybersicherheit, Datenschutz. Die EU schlägt Pflöcke für digitale Standortpolitik ein*, Berlin: Stiftung Wissenschaft und Politik, Juni 2013 (SWP-Aktuell 35/2013). Aktuelle Anregungen für Berichtsregeln, unter anderem für börsennotierte Unternehmen oder Betreiber kritischer Infrastruktur, hat der für die Beziehungen zu den USA verantwortliche EP-Abgeordnete Christian Ehler in Konsultation mit Experten des US-Senators John Rockefeller erarbeitet. Als Orientierungspunkt dient die Disclosure Guidance Initiative, die bereits einer ersten Bewertung durch die Vorsitzende der Securities and Exchange Commission, Mary Jo White, unterzogen wurde. Vgl. U.S. Securities and Exchange Commission, *Disclosure Guidance*, Washington, D.C., 16.7.2013, <www.sec.gov/divisions/corpfin/cfdisclosure.shtml>.

87 »Verordnung (EU) Nr. 611/2013 der Kommission vom 24. Juni 2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation)«, in: *Amtsblatt*, L 173, 26.6.2013, und »EU-Meldepflicht bei Datenklau tritt in Kraft«, *futurezone.at*, 25.8.2013.

88 »Sharp Increase in Cyberattacks on U.S. Critical Infrastructure«, *Homeland Security News Wire*, 3.7.2012.

Infrastruktur hingewiesen.[89] In der Cybersicherheit fehlt es jedoch auch weiterhin an einem einheitlichen europäischen Lagebild. Eine Meldepflicht für Sicherheitsvorfälle wird derzeit nicht nur in der EU und Deutschland, sondern auch den USA diskutiert.[90] Solange europaweit standardisiert erfasste Lagebilder fehlen, greift man auf einzelne staatliche[91] oder private[92] Bedrohungsanalysen zurück. Als zentral für die Bekämpfung der Cyberkriminalität und den Schutz kritischer Infrastrukturen gilt der Informationsaustausch zwischen Wirtschaft, Industrie, Behörden und Organisationen mit Sicherheitsaufgaben.

In den USA dreht sich die Cyberdebatte seit zwei Jahren immer stärker um den Schutz kritischer Infrastrukturen und die Rolle privater Unternehmen.[93] Nachdem es dem US-Senat nicht gelungen war, eine verbindliche gesetzliche Regelung zum Informationsaustausch über Cybergefahren durch das Repräsentantenhaus zu bringen, hat Präsident Barack Obama am 12. Februar 2013 eine Verordnung (executive order) zur Cybersicherheit erlassen.[94] Betroffene Unternehmen werden hier aufgefordert, staatliche Stellen zunächst freiwillig über Cyberattacken zu informieren.[95] Ende Februar 2013 hat der Cybersicherheitsbeauftragte im Weißen Haus, Michael Daniel, angekündigt, den gescheiterten Gesetzesvorschlag von 2012 zum Schutz kritischer Infrastrukturen wieder einzubringen. Im selben Monat versammelte Präsident Obama führende Vertreter der US-Wirtschaft, darunter UPS, JP Morgan Chase und Exxon Mobil, um Cyberbedrohungen zu erörtern. Auf diese Kooperationen ist der Präsident angewiesen, da die US-amerikanische digitale Infrastruktur von privaten Unternehmen betrieben wird. Als Vorbereitung auf die Gesetzesinitiative veröffentlichte die Administration im August 2013 das Cyber Security Framework (CSF) »of standards, guidelines, and best practices to promote the protection of critical infrastructure«, das verbindliche Schutzstandards empfiehlt. Es wurde vom National Institute of Standards and Technology nach Beratungen mit Stakeholdern aus Industrie, Wissenschaft und Regierung als Diskussionsgrundlage herausgebracht. Die endgültige Version soll im Februar 2014 folgen.[96]

Im Gegensatz zur Mehrheit im Repräsentantenhaus und im Einklang mit der US-Administration und dem US-Senat strebt die EU eine verbindliche Regulierung an.[97] Der aktuelle Richtlinienvorschlag der Kommission sieht vor, die Betreiber kritischer Infrastrukturen darauf zu verpflichten, den Schutz der von ihnen eingesetzten Informationstechnik und ihre Kommunikation mit dem Staat zu verbessern. Zu diesen kritischen Infrastrukturen zählt die Kommission nicht nur Energie- und Verkehrsunternehmen, sondern auch Suchmaschinen, Cloud-Computing-Dienste, soziale Netzwerke, Internet-Zahlungs-Gateways und Application Stores. Alle diese Unternehmen sollen der neuen Meldepflicht für IT-Sicherheitsvorfälle unterliegen, um Cyberkriminalität effizienter zu bekämpfen. Dafür, dass die erlangten Informationen vertraulich bleiben, sollen die ENISA auf europäischer und das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf nationaler Ebene sorgen.

Datenschutz

Das Verständnis von Sicherheit und Freiheit ist auf beiden Seiten des Atlantiks und innerhalb der EU sehr unterschiedlich ausgeprägt.[98] Der 11. September 2001

89 Vgl. »ENISA Reports on Most Frequent Cyber Threats in 2013«, in: *Bulletin Quotidien Europe*, (9.1.2013) 10759; Louis Marinos/Andreas Sfakianakis, *ENISA Threat Landscape*, Heraklion, 8.1.2013.

90 Ende Juni 2013 hat die EU eine Verordnung für Kommunikationsunternehmen erlassen, die am 25.8.2013 in Kraft trat. »Verordnung (EU) Nr. 611/2013« [wie Fn. 87].

91 In der operativen IT-Sicherheit in Europa und in Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) führend. Als zentraler IT-Sicherheitsdienstleister wendet es sich auch an die Hersteller sowie die privaten und gewerblichen Nutzer und Anbieter von Informationstechnik und ist für die operative Abwehr von Angriffen auf die IT-Infrastruktur zuständig. Mit Hilfe seiner Standards und Empfehlungen wirkt es auf die Cybersicherheit der Wirtschaft hin. Vgl. auch »ENISA Reports on Most Frequent Cyber Threats« [wie Fn. 89]; Deutsche Telekom/T-Systems (Hg.), *Cyber Security Report 2012. Ergebnisse einer repräsentativen Befragung von Entscheidungsträgern aus Wirtschaft und Politik*, 2012.

92 Z.B. die Adresse *www.sicherheitstacho.eu* der Deutschen Telekom.

93 U.S. Department of Homeland Security, *The Strategic National Risk Assessment in Support of PPD 8: a Comprehensive Risk-based Approach toward a Secure and Resilient Nation*, Washington, D.C., Dezember 2011.

94 The White House, *Executive Order: Improving Critical Infrastructure Cybersecurity*, Washington, D.C., 12.2.2013.

95 Siehe auch U.S. Department of Homeland Security, *National Infrastructure Protection Plan. Partnering to Enhance Protection and Resiliency*, Washington, D.C., 2009, <www.dhs.gov/national-infrastructure-protection-plan>.

96 National Institute of Standards, *Discussion Draft of the Preliminary Cybersecurity Framework*, 28.8.2013, <www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf> (Zugriff am 30.10.2013).

97 Vgl. Bendiek, *Kritische Infrastrukturen* [wie Fn. 86].

98 Jim Harper/Axel Spies, *A Reasonable Expectation of Privacy?*

war für die amerikanische Bevölkerung ein ebenso tiefer Schock wie die Anschläge in Madrid 2004 für Spanien und diejenigen in London im Juli 2005 für Großbritannien. Die unterschiedlichen Erfahrungen der EU-Staaten mit Terroranschlägen prägen ihre jeweiligen Herangehensweisen und einzusetzenden Mittel in der Terrorismusbekämpfung. Es herrscht große Uneinigkeit, ob und unter welchen Bedingungen es staatlichen Instanzen gestattet werden soll, zur Kriminalitätsbekämpfung auf private Daten zuzugreifen. Auch gehen die Vorstellungen darüber auseinander, ob und wie lange personenbezogene Daten jenseits der Strafverfolgung genutzt werden können und sollen.

Der vergleichsweise hohe Stellenwert von Sicherheitsfragen für die USA zeigt sich schlaglichtartig in den jüngst bekannt gewordenen Überwachungspraktiken der NSA (wie PRISM, Upstream, Xkeyscore oder Bullrun). Die US-Regierung hat in den letzten Dekaden eine umfassende militärisch-industrielle Sicherheitsarchitektur aufgebaut und den Sicherheitsdiensten weitestgehend freie Hand gelassen, alle ihr relevant erscheinenden Informationen zu erheben. Dass der US-Präsident – möglicherweise unwissentlich – Regierungsstellen der EU und ihrer Mitgliedstaaten verwanzen und sogar Telefone europäischer Regierungschefs abhören ließ, ist nur der offensichtlichste Ausdruck einer Sicherheitspraxis, die jedes Maß verloren zu haben scheint.

Die USA scheinen zudem noch immer wenig Einsicht dafür zu zeigen, wie hoch die politischen Kosten für das Ausspionieren ihrer Verbündeten sind. Das Überwachungsprogramm PRISM wird von der US-Administration mit dem Argument verteidigt, es werde nur zur gezielten Sammlung von Meta- und Inhaltsdaten eingesetzt und beziehe sich immer auf konkrete Personen, Gruppen und Ereignisse. Alle Maßnahmen seien zudem vom Foreign Intelligence Surveillance Act (FISA) gedeckt, unterlägen einer richterlichen Kontrolle durch das zuständige Fachgericht (FISA Court) und müssten dem Kongress berichtet werden.[99] Überdies weiche die US-Praxis kaum von vergleichbaren Aktivitäten europäischer Nachrichtendienste ab.[100] In der EU und vor allem in Deutschland ist der Unmut über die US-Praktiken in den letzten Monaten daher immer weiter angestiegen. Die Working Party 29 der EU, eine schon Mitte der neunziger Jahre eingerichtete intergouvernementale Arbeitsgruppe aus mitgliedstaatlichen und europäischen Datenschutzbeauftragten, prüft derzeit, ob von US-Seite Verstöße gegen internationale Rechtsnormen und die Budapester Konvention vorliegen.[101]

Der Umgang mit personenbezogenen Daten sorgt ebenfalls seit Jahren für Streit zwischen der EU und den USA. Das war beim Abkommen über die Ermittlung von Fluggastdaten (Passenger Name Record, PNR) an US-Behörden ebenso der Fall wie beim Austausch von Finanzdaten über den Dienstleister SWIFT (Abkommen über das Terrorist Finance Tracking Program, TFTP).[102] Bis heute beklagen Parlamentarier Probleme bei der Umsetzung des SWIFT-Abkommens durch die USA. Die Kritik reicht so weit, dass eine Aussetzung des Abkommens gefordert wird. Der Schutz personenbezogener Daten müsse gewährleistet bleiben, Abstriche bei Europas hohen Schutzstandards dürfe es auf keinen Fall geben, warnte das EP in einer Entschließung.[103]

Auch im Zuge der Verhandlungen über die Transatlantische Handels- und Investitionspartnerschaft (TTIP) sollte dafür Sorge getragen werden, dass EU-Datenschutzschutzstandards nicht ausgehöhlt werden. Die aktuell zur Reform stehende Datenschutzrichtlinie aus dem Jahr 1995 verbietet es, personenbezogene Daten aus EU-Mitgliedstaaten in Länder zu übertragen, die nicht über einen dem europäischen Recht vergleichbaren Datenschutz verfügen. Dazu gehören auch die USA. Mit der im Jahr 2000 zwischen EU und USA geschlossenen Datenschutzvereinbarung »Safe Harbor« jedoch konnten sich US-Unternehmen

Data Protection in the United States and Germany, Washington, D.C.: American Institute for Contemporary German Studies (AICGS), 2006 (AICGS Policy Report Nr. 22); vgl. Daniela Kietz/Johannes Thimm, *Zwischen Überwachung und Aufklärung. Die amerikanische Debatte und die europäische Reaktion auf die Praxis der NSA*, Berlin: Stiftung Wissenschaft und Politik, August 2013 (SWP-Aktuell 51/2013); vgl. grundlegend Quirine Eijkman/Daan Weggemans, »Open Source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability?«, in: *Security and Human Rights*, (2012) 4, S. 285–296.

99 Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Washington, D.C., 8.6.2013.

100 Vgl. Georg Mascolo/Ben Scott, *Lessons from the Summer of Snowden. The Hard Road Back to Trust*, Washington, D.C.: Open Technology Institute/Wilson Center, Oktober 2013.

101 »Article 29 Group to Carry Out Its Own Espionage Investigation«, in: *Bulletin Quotidien Europe*, (21.8.2013) 10903.

102 Annegret Bendiek, *An den Grenzen des Rechtsstaates: EU-USA-Terrorismusbekämpfung*, Berlin: Stiftung Wissenschaft und Politik, Februar 2011 (SWP-Studien 3/2011).

103 Sophie in't Veld/Guy Verhofstadt, »Europe Must Get Tough with the US over NSA Spying Revelations«, in: *The Guardian*, 2.7.2013.

auf die »Grundsätze des sicheren Hafens« verpflichten lassen, um Daten aus Europa in den USA weiterzuverarbeiten. Die australische Datenschutz-Beratungsfirma Galexia hat in ihrer Untersuchung vom September 2013 festgestellt, dass die Richtlinie in den USA oft nicht beachtet wird. Die Forscher hatten knapp 3000 US-Firmen, die sich dem Safe-Harbor-Abkommen unterworfen haben, unter die Lupe genommen und 427 Verstöße gegen das Abkommen gefunden. Bei der vorigen Untersuchung im Jahr 2008 waren es nur 200 gewesen.[104] Das Safe-Harbor-Abkommen umfasst datenschutzrelevante Handels- und Wirtschaftsaspekte und wird daher getrennt von den EU-USA-Abkommen behandelt, die im Rahmen der Strafverfolgung (PNR, SWIFT, aber auch Rechtshilfeabkommen) gültig sind.

In den neuen Entwurf zur EU-Datenschutzverordnung fügte das EP die sogenannte Anti-FISA-Klausel wieder ein. Die Kommission hatte diese zuvor auf Druck der US-Regierung gestrichen.[105] Die Klausel besagt, dass Unternehmen sensible Daten von EU-Bürgern nur noch dann ausländischen Sicherheitsbehörden übermitteln dürfen, wenn dies durch ein Rechtshilfeabkommen gedeckt ist. Solange sich die USA und die EU nicht auf neue Regeln für den Datenaustausch einigen, müssten Unternehmen der US-Regierung die Herausgabe verweigern. Solche Rechtsunsicherheit bringt Firmen wie etwa Facebook in Schwierigkeiten. Die von der Überwachung betroffenen Firmen haben daher in offenen Briefen die US-Regierung um Erlaubnis gebeten, alle Anfragen der Geheimdienste nach Nutzerdaten öffentlich zu machen und die bisherigen NSA-Praktiken zu beenden. Bis Ende 2014 wollen die Justizminister der Mitgliedstaaten und das EP einen endgültigen Entwurf verabschieden, der 2016 in Kraft treten könnte. Die Kommissarin für Justiz, Grundrechte und Bürgerschaft, Viviane Reding, hat sich dafür ausgesprochen, vier wesentliche Bausteine eines europäischen Datenschutzsystems beizubehalten: Erstens müsse der territoriale Anwendungsbereich der Vorschriften klar festgelegt werden. Demnach sollen Unternehmen außerhalb Europas die EU-Datenschutzvorschriften vollständig erfüllen, wenn sie Produkte und Dienstleistungen auf dem europäischen Markt anbieten möchten. »Wer in unserem Hof spielen möchte, muss auch unsere Spielregeln befolgen«,[106] so Reding. Zweitens solle der Begriff der personenbezogenen Daten weiter gefasst werden. Er solle sich nicht nur auf die Inhalte von E-Mails und Telefongesprächen beziehen, sondern auch auf die damit verbundenen Verkehrsdaten, von denen aus etwas versendet wurde. Drittens müssten diese Vorschriften nicht nur für Unternehmen gelten, die Daten von Bürgern erheben, sondern auch für Dienstleverarbeiter, wie zum Beispiel Cloud-Anbieter. Und viertens schließlich müsse es auch einen Schutz vor uneingeschränkten internationalen Datenübertragungen geben. Daten von EU-Bürgern sollen nur in genau definierten Ausnahmesituationen und unter gerichtlicher Kontrolle an nichteuropäische Strafverfolgungsbehörden übermittelt werden dürfen.

Nicht zuletzt wurden die Verhandlungen über ein Grundsatzabkommen zu den Modalitäten des Datenschutzes zwischen der EU und den Vereinigten Staaten (umbrella agreement) wieder aufgenommen. Es soll das Recht der Bürger stärken, auf eigene Daten zugreifen zu können und sie gegebenenfalls berichtigen oder sogar löschen zu lassen. Auch sollen EU-Bürger das Recht erhalten, gegen eine unrechtmäßige Verarbeitung ihrer Daten in den USA zu klagen. Die Verhandlungen zu einem übergreifenden Datenschutzabkommen dürften davon profitieren, dass die US-Öffentlichkeit sich immer mehr für das Thema sensibilisiert. Die Frage des Schutzes personenbezogener Daten und die Kritik an den Überwachungspraktiken der Geheimdienste gewinnen zusehends an innenpolitischer Virulenz. Quer durch die politischen Lager,[107] aber auch in ersten richterlichen Stellung-

104 Chris Connolly, *The US Safe Harbor – Fact or Fiction?*, Sydney: Galexia, Dezember 2008; Chris Connolly, *EU/US Safe Harbor – Effectiveness of the Framework in Relation to National Security Surveillance*, 7.10.2013 (Papier für das Hearing im LIBE-Ausschuss); Konrad Lischka, »Prüfbericht zu Safe Harbor. US-Konzerne täuschen EU-Bürger beim Datenschutz«, in: *Spiegel Online*, 8.10.2013.

105 Siehe hierzu European Centre for International Political Economy, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, März 2013. Vgl. Wolfgang Böhm, »›Dreiste‹ Intervention der US-Lobby in Brüssel«, in: *Die Presse.com*, 21.2.2013.

106 Viviane Reding, »Reform durchsetzen«, in: *Handelsblatt*, 13.10.2013, S. 48. Eine kritische und aufschlussreiche Auseinandersetzung mit den europäischen Vorschlägen bietet Kapitel 5 (»Datenpolitik«) in: Baums/Scott (Hg.), *Digitale Standortpolitik* [wie Fn. 13].

107 Zwei Republikaner aus dem Repräsentantenhaus, Justin Amash und F. James Sensenbrenner, und der demokratische Senator Ron Wyden sind sich in ihrer Kritik einig und stellen öffentlich in Frage, dass der Kongress in seiner Funktion als Machtausgleich zur Regierung noch ernst zu nehmen ist. So auf der Konferenz des Cato-Instituts »NSA Surveillance: What We Know; What to Do about It?«, Washington, D.C., 9.10.2013. Eine empfehlenswerte Lektüre zu den jüngsten Gesetzesvorschlägen »USA Freedom Act« und »Intelligence Oversight and Surveillance Reform Act« sind die Analysen von Jennifer

nahmen[108] wird bezweifelt, dass die gigantischen Datensammlungen der NSA notwendig sind und dazu beitragen können, die Amerikaner vor terroristischen Anschlägen zu schützen. Hingewiesen wird auch darauf, dass der Zugriff der Geheimdienste auf die Daten US-amerikanischer Hightech-Firmen deren Reputation gefährde und mittelfristig massive ökonomische Konsequenzen haben könnte. Es bleibt abzuwarten, welche der 46 Reformvorschläge, die die von Präsident Obama eingesetzte Expertengruppe zur US-amerikanischen Geheimdienstarbeit unterbreitet hat, in den nächsten Monaten auch umgesetzt werden.[109]

Transnationale Konflikte

Der Konflikt zwischen den USA und der EU über Fragen des Datenschutzes ist politisch so brisant, weil er direkten Einfluss auf das innenpolitische Verhältnis zwischen Regierungen und Bürgern hat. Beim Datenschutz geht es nicht nur um internationale, sondern immer auch um innerstaatliche Politik und die Gestaltung öffentlicher Ordnung. Auf die Dauer wird die transatlantische Partnerschaft daher nur stabil bleiben können, wenn sie auf einem festen gesellschaftlichen Fundament aufbaut. Doch diese Basis bröckelt. Die Cyberpolitiken der USA und der EU geraten in einen wachsenden Widerspruch zu zentralen Bürgerrechten, zu Fragen der menschlichen Sicherheit und der freien Nutzung von Inhalten im Internet. Hier findet sich langfristig die sicherlich größte Bedrohung der transatlantischen Cyberpartnerschaft.

Bürgerrechte in der Defensive

Der zentrale Konflikt in Bezug auf die Praktiken der NSA verläuft daher auch nicht nur zwischen den USA und betroffenen europäischen Regierungen, sondern ebenfalls zwischen betroffenen Bürgern und ihren Regierungen.[110] Es scheint sich eine transatlantische intergouvernementale Praxis der Erhebung und Auswertung privater Kommunikationsdaten etabliert zu haben, die in Widerspruch zu grundlegenden Bürgerrechten steht.[111] Auffällig ist, dass die Überwachungsprogramme der beiden Nachrichtendienste NSA und GCHQ (Government Communications Headquarters) auf relativ wenig Protest seitens der betroffenen Regierungen gestoßen sind.[112] Die Analysesoftware Xkeyscore wird nicht nur von der NSA, sondern auch vom Bundesnachrichtendienst genutzt. Das Bundesamt für Verfassungsschutz erhielt nach eigenen Angaben eine Testversion. Die Bundesregierung verteidigte die US-Praktiken sogar mit dem Hinweis, dass die NSA lediglich »eine gezielte Sammlung der Kommunikation Verdächtiger in den Bereichen organisierte Kriminalität, Weiterverbreitung von Massenvernichtungswaffen und zur Gewährleistung der nationalen Sicherheit der USA«[113] vornehme. Sie beruft sich hierbei auf die Auskunft der Amerikaner und stellt fest, dass Bundesbürger nicht flächendeckend ausgespäht würden.[114]

Die Privatisierung von Datenwissen wird heute von einer interessierten Öffentlichkeit auf beiden Seiten des Atlantiks kritisch gesehen. Der einst mächtige westliche Mythos von der separaten virtuellen Welt, in der es mehr Privatheit und größere Unabhängigkeit von gesellschaftlichen und politischen Einrichtungen

Granick (Center for Internet and Society, Stanford Law School), <cyberlaw.stanford.edu/about/people/jennifer-granick>.

108 Siehe z.B. Ellen Nakashima/Ann E. Marimow, »Judge: NSA's Collecting of Phone Records is Probably Unconstitutional«, in: *The Washington Post*, 16.12.2013; »Geheimdienstskandal: NSA-Telefonüberwachung laut US-Richter wohl verfassungswidrig«, in: *Spiegel Online*, 16.12.2013.

109 David E. Sanger/Charlie Savage, »Obama Panel Recommends New Limits on N.S.A. Spying«, in: *The New York Times*, 18.12.2013, <www.nytimes.com/2013/12/19/us/politics/report-on-nsa-surveillance-tactics.html>.

110 Laura Poitras/Marcel Rosenbach/Holger Stark, »Codename ›Apalachee‹: How America Spies on Europe and the UN«, in: *Der Spiegel*, (26.8.2013) 35, S. 85–89; vgl. Nicole Perlroth/Jeff Larson/Scott Shane, »N.S.A. Able to Foil Basic Safeguards of Privacy on Web«, in: *The New York Times*, 5.9.2013.

111 Vgl. Stefan Heumann/Ben Scott, *Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany*, Berlin: Stiftung Neue Verantwortung, September 2013; vgl. Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz u.a., »Geheime Kooperationsprojekte zwischen deutschen und US-Geheimdiensten«, Berlin: Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/14759, 16.9.2013.

112 »Wir wollen überwacht werden!«, in: *Frankfurter Allgemeine Zeitung*, 15.9.2013, S. 55.

113 Siehe zu den gegenteiligen Positionen Anträge der Fraktionen von SPD (17/14677), Die Linke (17/14679) und Bündnis 90/Die Grünen (17/14676), in: *heute im bundestag* (hib), (3.9.2013) 444.

114 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko u.a., »Weltweite Ausforschung der Telekommunikation über das US-Programm PRISM«, Berlin: Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/14602, 22.8.2013.

gebe,[115] wird immer mehr in Frage gestellt. In einer Welt grenzüberschreitender Kommunikationsflüsse können nationale und europäische Rechtsordnungen, etwa zur Vorratsdatenspeicherung, und national garantierte Grundrechte nur für wenig Sicherheit sorgen. Innerhalb der EU besteht das größte Problem darin, dass EU-Staaten die Vorratsdatenspeicherung nicht nur zur Bekämpfung des Terrorismus und schwerer Kriminalität benutzen. Nach der E-Privacy-Richtlinie[116] können solche Daten auch für andere, inhaltlich kaum klar abgrenzbare Zwecke verwendet werden, wie die Verbrechensvorbeugung oder die Gewährleistung der öffentlichen Ordnung.[117] Auch die beiden wichtigsten transatlantischen Rechtsdokumente für die Bekämpfung von Kriminalität (Budapester Konvention) und die Übertragung völkerrechtlicher Normen aus dem Kriegsrecht auf die Cyberpolitik (Tallinn Manual) verraten wenig Sensibilität für Bürgerrechte.

Die Budapester Konvention ist unter Menschenrechtlern und Datenschützern höchst umstritten. Artikel 16 der Konvention sieht vor, dass gespeicherte Computerdaten 90 Tage vom Dienstanbieter vorzuhalten sind, damit die Strafverfolgungsbehörden bei einem eventuellen Kriminalfall mit Hilfe üblicher Ermittlungs- und Rechtshilfemaßnahmen auf diese Daten zugreifen können. Auf Wunsch einer Vertragspartei kann die Speicherung auch verlängert werden. Außerdem ist es den Vertragsstaaten möglich, eine Echtzeitüberwachung der Verkehrs- und Verbindungsdaten und auch der Inhalte bereitzustellen. Bei einem Anfangsverdacht müssen Dienstanbieter persönliche Informationen über ihre Kunden an die Strafverfolgungsbehörden herausgeben. Amerikanische Anbieter erlauben US-Behörden den Zugriff auf Daten selbst dann, wenn diese in Europa gespeichert werden. Was der eine Dienst in seinem jeweiligen Inland nicht überwachen darf oder kann, erledigt der befreundete Partnergeheimdienst und teilt dann seine Erkenntnisse mit.

Auch das Tallinn Manual erntete viel Kritik. Die weit gefasste Definition eines kriegerischen Angriffs schließt nicht grundsätzlich aus, dass staatliche Organe militärische Maßnahmen gegen nichtstaatliche Gruppen oder sogar einzelne (mutmaßliche) Hacker ergreifen. Auf diese Weise, so die Befürchtung, wird die Kriegsführung entstaatlicht, und die Grenzen zwischen polizeilichen und militärischen Maßnahmen verschwimmen immer mehr. Da militärische Handlungsabläufe keine rechtsstaatlichen Garantien und einen nur sehr eingeschränkten Grundrechteschutz kennen, besteht die Gefahr, dass die Logik des Drohnenkriegs im Kampf gegen den Terror auf die Cyberdefencepolitik übertragen werden könnten.

Bemerkenswert ist, dass die transatlantische Cyberpartnerschaft eine stark intergouvernementale Dimension hat und die Einbindung der Zivilgesellschaft vernachlässigt. Gouvernementale Handlungsrationalitäten und bürgerrechtliche Garantien beginnen auseinanderzufallen. Ein Paradebeispiel hierfür sind die unterschiedlichen Auffassungen darüber, wie man mit Edward Snowden umzugehen habe.[118] Wo Regierungen Sicherheitsprobleme wahrnehmen und mit der Aneignung neuer Kompetenzen reagieren, da entstehen gleichzeitig Gefährdungen der Zivilgesellschaft.[119] Es kann daher auch nicht erstaunen, dass bereits die ersten Klagen zivilgesellschaftlicher Organisationen gegen Regierungshandeln beim Europäischen Gerichtshof für Menschenrechte anhängig sind. Drei der angesehensten britischen zivilgesellschaftlichen Organisationen (Big Brother Watch, Open Rights Group und der englische PEN) haben eine Klage gegen Großbritannien eingereicht, da die Abhörpraktiken des GCHQ ihrer Auffassung nach gegen Artikel 8 der Europäischen Menschenrechtskonvention verstoßen. Die breit angelegte und verdachtsunabhängige Erhebung von Kommunikationsdaten britischer Bürger verletze das Recht auf Schutz der Privatsphäre.[120]

115 Eric Schmidt/Jared Cohen, *Die Vernetzung der Welt*, Reinbek 2013.

116 »Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz«, in: *Amtsblatt*, L 337, 18.12.2009; »Berichtigung der Richtlinie 2009/136/EG«, in: *Amtsblatt*, L 241, 10.9.2013.

117 Vgl. »Im Gespräch: EU-Innenkommissarin Cecilia Malmström«, in: *Frankfurter Allgemeine Zeitung*, 4.7.2013.

118 Nikolaj Nielsen, »Snowden to EU: Whistleblowers Need Protection«, *EUobserver*, 1.10.2013.

119 Vgl. hierzu exemplarisch »Wenn die Macht schweigt. Ilija Trojanow, Juli Zeh und der Geheimdienst im Netz«, in: *Süddeutsche Zeitung*, 4.10.2013, S. 11; John Lanchester »The Snowden Files: Why the British Public Should Be Worried about GCHQ«, in: *The Guardian*, 3.10.2013; Ken Auletta, »Freedom of Information. A British Newspaper Wants to Take Its Aggressive Investigations Global, but Money Is Running Out«, in: *The New Yorker*, 7.10.2013.

120 Constanze Kurz, »Die Menschenrechte sollen es richten«, in: *Frankfurter Allgemeine Zeitung*, 4.10.2013, S. 38.

Auch in den USA sind noch einige Klagen gegen die NSA-Überwachungspraktiken anhängig.

Menschliche Sicherheit in der Defensive

Rüstungsunternehmen versuchen immer häufiger, mit Produkten aus dem Bereich der Cybersicherheit Einbußen zu kompensieren, die ihnen durch die öffentlichen Sparprogramme der letzten Jahre entstehen.[121] Sie sichern Netzwerke, bauen Firewalls und simulieren Hackerangriffe. Die Verkäufe von Cybersicherheit wachsen derzeit jährlich um zehn Prozent.[122] Rüstungsfirmen kaufen spezialisierte Technologieunternehmen auf und sichern sich damit die Dienste von Softwareexperten. Der US-Konzern Raytheon hat seit 2007 elf IT-Firmen übernommen, zuletzt Teligy, ein Unternehmen, das auf drahtlose Kommunikation spezialisiert ist.[123] Im Gegensatz zur traditionellen Waffenbranche konkurrieren Rüstungsfirmen mit zivilen Hightech-Konzernen wie Intel oder Dell um die beste IT-Sicherheit. Der Rüstungskonzern Cassidian plant, die Zahl seiner Cyberexperten in den kommenden Jahren auf 700 zu erhöhen. Der Ausbau der IT-Defensive bedeutet auch, dass sich die Grenzen zwischen zivilen und militärischen Unternehmen immer mehr verwischen. So will der britische Rüstungskonzern BAE mit dem Mobilfunkanbieter Vodafone kooperieren.[124]

Die Menschenrechtsorganisation Privacy International hat weltweit rund 160 Unternehmen erfasst, deren Softwareprodukte auch zur Überwachung oder Unterdrückung von Oppositionellen benutzt werden können.[125] Ein Großteil der Unternehmen ist in Europa und den USA ansässig. Mit dem Export ihrer Software unterstützen sie Autokraten in der ganzen Welt darin, die freie Meinungsäußerung zu unterbinden und Menschenrechte zu verletzen. Die Ausbreitung der Demokratie wird damit behindert, die nachhaltige Stabilisierung der internationalen Umwelt unterminiert. Wenn Firmen unsichere Software auf den Markt bringen, erleichtert dies auch die Überwachung seitens autoritärer Staaten.[126] Dass Technologie zur Förderung von Cybersicherheit genauso moralische Fragen aufwirft wie die traditionelle Waffentechnik, zeigt das Beispiel der Firma Gamma International mit Sitz in München. Sie entwickelt und vertreibt einen Trojaner namens FinFisher, der Computer ausspähen und Mobiltelefone abhören kann. Das Unternehmen verkauft das Programm mit Hilfe anderer Firmen weltweit an Polizei und Geheimdienste. Menschenrechtler werfen Gamma International vor, auch an Diktaturen zu liefern. Die Firma hält dem entgegen, dass sie vor jedem Verkauf die Exportverbotslisten Deutschlands, Großbritanniens und der USA konsultiert.[127] Gamma International ist nicht das einzige Unternehmen, dessen Geschäftspraxis in der Kritik steht. Der schwedische Telekommunikationskonzern TeliaSonera exportierte seine Erzeugnisse in Nachfolgestaaten der Sowjetunion. Und der Netzwerkausrüster BlueCoat, eine US-Firma, lieferte Überwachungstechnik in zahlreiche Staaten, die entweder US-Sanktionen unterliegen, wie Iran, Syrien, Sudan, Nordkorea oder Kuba, oder in denen massive Menschenrechtsverletzungen begangen und Oppositionelle unterdrückt werden, wie Ägypten, Bahrain, Kuwait und Saudi-Arabien.

Kritiker sind deshalb der Meinung, dass Reformen der Exportkontrolle sensibler Software sowohl die exportierenden Unternehmen als auch die Exportkontrollregime in den EU-Staaten stärker in die Verantwortung nehmen müssen.[128] Die Electronic Frontier Foundation, Citizen Lab und Privacy International haben wichtige Vorschläge unterbreitet, um die Kontrollen zu verbessern: Unternehmen sollen kritische Software nur in Länder ausführen dürfen, die die Menschenrechte beachten beziehungsweise der Opposition freie und ungehinderte Meinungsäußerung zugestehen. Nach diesem Vorschlag bildet die Einhaltung von Menschenrechtsstandards die

121 Vgl. Stockholm International Peace Research Institute (SIPRI), *SIPRI Yearbook 2013*, Stockholm u.a., 2013, 3. Kapitel (Military Expenditure), Punkt I (Global Developments in Military Expenditure). Dem in die Hände spielt auch das neue europäische Vergaberecht für den Rüstungsbereich, vgl. Heiko Höfler/Christine Herkommer, »Der Entwurf liegt vor. Das neue Vergaberecht für den Rüstungsbereich«, in: *Behörden Spiegel*, Juli 2012, S. 29.

122 *Cyber Security M & A. Decoding Deals in the Global Cyber Security Industry*, PricewaterhouseCoopers, November 2011, S. 5.

123 Ryan Gallagher, »Software That Tracks People on Social Media Created by Defence Firm«, in: *The Guardian*, 10.2.2013.

124 Nach jüngsten Zahlen verlor BAE 2012 in fast allen traditionellen Sparten. »A Strategic Partnership with Vodafone«, *BAESystems*, 17.2.2013.

125 Privacy International, Projekt »Global Surveillance Monitor«. Vergleichbar ist auch der Surveillance Catalog des Wall Street Journal.

126 Vgl. »Russland plant die totale Überwachung im Internet«, in: *Deutsche Wirtschafts Nachrichten*, 21.10.2013.

127 Hanna Lütke-Lanfer, »Ein Trojaner für den König«, in: *Die Zeit*, 14.2.2013.

128 Vgl. Wolfgang Ischinger, »Mehr Macht dem Parlament«, in: *Handelsblatt*, 30.8.2012, S. 56.

Voraussetzung dafür, dass eine Nutzungslizenz auf Zeit erteilt werden kann. Stellt sich später heraus, dass die Menschenrechte verletzt werden, müsse die Lizenz wieder entzogen werden. Angeregt wurde auch, jede Software mit einem Label zu versehen, das ausweist, wofür sie im Detail verwendet werden darf. Auf dieser Grundlage könnten Unternehmen auf den Nachweis verpflichtet werden, dass die Software zweckgebunden eingesetzt wird. Zusätzlich könnten einzelne Überwachungsinstrumente wie Trojaner als digitale Waffe eingestuft und damit einer strikten Genehmigungspflicht unterworfen werden.

Die bisherigen Exportkontrollen reichen nicht aus und müssen an die Entwicklung digitaler Technologie angepasst werden.[129] Die Obama-Administration erließ im April 2012 eine Verordnung (executive order), um die Ausfuhr von Informations- und Kommunikationstechnologie nach Iran und Syrien zu unterbinden. Auch die EU verhängte ein Embargo über Syrien. Zudem hat die US-Regierung Exportkontrollen für Programme angeordnet, die heimliche Lauschangriffe (surreptitious listening) ermöglichen. Die EU hat zwar untersagt, Güter mit doppeltem Verwendungszweck (sogenannte Dual-use-Güter, also Gegenstände, Technologien und Kenntnisse, die sowohl zivilen als auch militärischen Zwecken dienen können) in Länder zu exportieren, die einem Waffenembargo unterliegen. Systematische Vorabkontrollen im Hinblick auf die Menschenrechtslage in Empfängerländern sind aber in diesem Bereich nicht vorgeschrieben. Das EP hat sich im September 2011 dafür ausgesprochen, die Exportregeln für Überwachungstechnik, vor allem für die Ausfuhr von Dual-use-Gütern, zu verschärfen. Einzelne Staaten wie die Niederlande und Dänemark haben vorgeschlagen, den Export sensibler Güter von einer verpflichtenden Überprüfung von Menschenrechts- und Demokratiebedingungen und strikteren Kontrollmechanismen abhängig zu machen. In ihrer Stellungnahme von Ende Oktober 2011 zum Grünbuch der Europäischen Kommission zum EU-Ausfuhrkontrollsystem von Dual-use-Gütern fordert die Bundesregierung ausdrücklich, dass »zukünftig sowohl ›außen- und sicherheitspolitische Interessen‹ als auch ›die Interessen der Wirtschaft‹ [...] ›ausgewogen Berücksichtigung finden‹ sollen«.[130] Wirksame Maßnahmen zur Anpassung an politische und technische Entwicklungen wollen die EU-Staaten vorrangig auf internationaler Ebene treffen.[131] Die Bundesregierung wirkt im Rahmen des Wassenaar-Arrangements aktiv an diesen Verhandlungen mit.[132]

Nutzungsfreiheiten versus Urheberrechte

Es gibt eine wachsende Gruppe von Kritikern, die befürchten, dass die Freiheit des Internets zunehmend der Logik globaler Marktverwertung unterworfen wird. Symptomatisch für diese Debatte war die bis 2012 geführte Auseinandersetzung über das Anti-Counterfeiting Trade Agreement (ACTA). Die ACTA-Saga begann 2007, als EU und USA erklärten,[133] international gegen Produkt- und Markenfälschungen vorgehen zu wollen, gemeinsam mit Ländern wie Japan, Kanada, Korea, Marokko, Mexiko, Neuseeland oder der Schweiz im Rahmen eines Handelsabkommens. Das Abkommen sollte einen besseren Schutz für die Vermarktung immaterieller Güter sicherstellen. Zudem sollten Verbraucher vor Gesundheits- und Sicherheitsrisiken bewahrt werden, die mit einigen gefälschten Produkten wie etwa nachgemachten Medikamenten verbunden werden. Nachdem diese ursprüngliche Idee auf das Internet und die Bekämpfung von Urheberrechtsverletzungen im Netz ausgeweitet worden war, gewann ACTA spürbar an politischer Brisanz. Das Abkommen sah teilweise empfindliche Strafen vor, die bis zur Sperrung des Internetzugangs reichen sollten. Viele Protestler sahen in dem Vertrag zudem ein Symbol für die ständige Ausweitung des Systems des »geistigen Eigentums«, das die Anpassung des Urheberrechts an die Belange der digitalen Gesellschaft verhindert. Als die Proteste immer größeren Zulauf erhielten, lehnte das EP das Abkommen im Juli

129 Danielle Kehl/Tim Maurer, *Against Hypocrisy: Updating Export Controls for the Digital Age*, Washington, D.C./New York: New America Foundation, 9.3.2013.

130 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz u.a., »Haltung der Bundesregierung bezüglich des Exports von ›Dual-use-Gütern‹ im Bereich der Technologie zur Störung von Telekommunikationsdiensten sowie Techniken zur Überwachung und Unterbrechung des Internetverkehrs durch deutsche Firmen«, Berlin: Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/8052, 2.12.2011, S. 2.

131 U.S. Department of Commerce, Bureau of Industry and Security, *2013 Report on Foreign Policy-based Export Control*, Washington, D.C., 2013.

132 Siehe hierzu die offizielle Webseite, <www.wassenaar.org>. Vgl. Guido Westerwelle/Ewa Björling/Laurent Fabius/William Hague, »So muss der Waffenhandel global reguliert werden«, in: *Financial Times Deutschland*, 2.7.2012, S. 24.

133 Stefan Krempl, »EU und USA treiben Abkommen gegen Produktpiraterie voran«, *heise.de*, 24.10.2007.

2012 ab. Damit gilt der von führenden Industrienationen vorangetriebene und weitgehend hinter verschlossenen Türen ausgehandelte Vorstoß sowohl in Europa wie auch international als gescheitert.[134]

In der aktuellen Debatte über die Transpazifische Partnerschaft (TPP) und die Transatlantische Handels- und Investitionspartnerschaft (TTIP) tauchen viele der schon zu ACTA geäußerten Befürchtungen wieder auf.[135] Auch die TTIP sieht einen transatlantischen Schutz im Patent- oder Urheberrecht vor und zudem wahrscheinlich auch ein Streitbeilegungsverfahren, mit dem Konzerne Nationalstaaten wegen missliebiger Klauseln verklagen könnten. Das Investor-State Dispute Settlement (ISDS) wurde ursprünglich geschaffen, um Investoren in Staaten mit mangelnder Rechtsstaatlichkeit vor willkürlichen Regierungsauflagen und Gerichtsentscheidungen zu schützen. Inzwischen nutzen aber vor allem US-Konzerne das Verfahren. Über die vorgelegten Fälle wird zumeist unter Ausschluss der Öffentlichkeit entschieden. Eine Berufungsinstanz ist nicht vorgesehen. Das Netzwerk »Seattle to Brussels« warnt in seinem Bericht mit dem Titel »A Brave New Transatlantic Partnership«, dass das Abkommen den »Geist von ACTA« wiederbeleben könne.[136] Die US-Seite binde Industrieverbände umfassend in die Verhandlungen ein, während die kritische Öffentlichkeit keinerlei Informationen erhalte.

Auch der Förderverein für eine Freie Informationelle Infrastruktur (FFII) lehnt das Verfahren ab.[137] Firmen könnten sich so gegen stärkere Nutzerrechte im Urheberrechtsgesetz oder die derzeit diskutierten »Fair Use«-Regelungen wenden. Im US-Copyright erlaubt die »Fair Use«-Klausel ganz allgemein solche Nutzungshinweise, die herkömmliche Verwertungsketten nicht gefährden. Die EU-Urheberrechtslinie (InfoSoc-RL) hingegen gewährt in Artikel 5 den Mitgliedstaaten nur in den ausdrücklich angeführten Fällen Ausnahmen vom urheberrechtlichen Schutz. Die Folgen dieser in Europa stärker beschränkten Nutzungsfreiheiten sind bisher allerdings weniger ein Problem für die Endnutzer, sondern weitaus mehr für innovative Unternehmen. Denn die meisten Verwertungsgesellschaften und Rechteinhaber sind klug genug, Bagatellverstöße von Einzelpersonen gegen das Urheberrecht nicht zu verfolgen. Stattdessen werden direkt jene Firmen angegangen, deren Dienstleistungen auf die eine oder andere Weise solche Verletzungen ermöglichen. Viele innovative Dienstleistungen entstehen daher eher in den USA als in Europa.[138]

134 Vgl. Stefan Krempl, »EU Parlament beerdigt ACTA«, *heise.de*, 4.7.2012.

135 Vgl. Stefan Krempl, »Transatlantisches Freihandelsabkommen: ›Schlimmer als ACTA‹«, *heise.de*, 11.10.2013.

136 Vgl. Kim Bizzarri, *A Brave New Transatlantic Partnership*, Brüssel: Seattle to Brussels Network, Oktober 2013, <www.s2bnetwork.org/fileadmin/dateien/downloads/Brave_New_Atlantic_Partnership.pdf>.

137 »FFII Condemns Investor-to-state Arbitration in Trade Talks with US«, *FFII Acta Blog*, 14.6.2013.

138 Vgl. Leonhard Dobusch, »Urheberrecht: Standortfaktor für digitale Innovationsoffenheit«, in: Baums/Scott (Hg.), *Digitale Standortpolitik* [wie Fn. 13], S. 116f.

Perspektiven transatlantischer Kooperation

Die transatlantische Cyberpartnerschaft ist umstritten. Zwar steht sie auf einem starken gemeinsamen Fundament von Prinzipien und Institutionen, darf aber nicht als eine von politischer Auseinandersetzung unabhängige Größe missverstanden werden. Ihre langfristige Stabilität wird vielmehr davon abhängen, dass beide Seiten das offene Gespräch suchen und eine Reihe gravierender Differenzen in Problemwahrnehmung und Problembearbeitung überwunden werden können. In der Cybersicherheit, dem Datenschutz, der Debatte über die Internet Governance und der Frage nach den Grenzen legitimer Überwachung unter Verbündeten wird es darauf ankommen, dass beide Partner sich als wirklich gleichwertig anerkennen und die USA sich von der überholten Idee verabschieden, einseitig Regeln für angemessenes Verhalten aufstellen zu können. Zugleich gilt es für die Europäer, eine gemeinsame Position zu allen diesen Fragen zu entwickeln und geeint gegenüber den USA aufzutreten.

Beide Seiten müssen sich zudem darüber im Klaren sein, dass die Vorstellung eines freien und offenen Internet sich nur dann wird aufrechterhalten lassen, wenn die gemeinsamen Governancestrukturen auch mit gemeinsamen Inhalten gefüllt werden. Alle Forderungen autoritärer Staaten nach verstärkter staatlicher Kontrolle kritischer Inhalte müssen einhellig zurückgewiesen werden. Dafür müssen die USA, die EU und andere demokratische Staaten besonders eng zusammenarbeiten, denn nur zusammen sind sie in der Lage, weltweit Standards zu setzen und die Offenheit und Freiheit des Internet zu bewahren. In der Internet Governance können die USA ihre Ziele nicht ohne Europa und Europa seine Ziele nicht ohne die USA realisieren. Das ist heute so und wird sich in den kommenden Jahren noch weiter verfestigen.

Eine große Herausforderung ist der Neuaufbau verlorengegangenen Vertrauens. Die Aufdeckung transatlantischer Spionagepraktiken der NSA hat das intergouvernementale Vertrauensverhältnis in der transatlantischen Zusammenarbeit nachhaltig erschüttert. Eine deutliche Sprache spricht hier der Vorstoß Brasiliens und Deutschlands, dem Internationalen Pakt über bürgerliche und politische Rechte Bestimmungen hinzuzufügen, um nationale Daten vor internationaler Ausspähung zu schützen. Zwei der wichtigsten Verbündeten der USA halten es für nötig, internationale Rechtsnormen so anzupassen, dass den USA Schranken gesetzt werden. Das ist nichts weniger als eine tiefe Vertrauenskrise in der transatlantischen Partnerschaft. Mittelfristig wird es daher notwendig sein, dass der enge Kreis der »Five Eyes« (USA, Großbritannien, Kanada, Australien, Neuseeland) um weitere ausgewählte Nato-Staaten erweitert wird. Dabei müssen die europäischen Staaten bestrebt sein, eine Kluft zwischen eingebundenen und nicht eingebundenen Staaten zu verhindern. Es wäre dem europäischen Integrationsprojekt in höchstem Maße abträglich, wenn sich eine europäische Zweiklassengesellschaft aus informierten und uninformierten Mitgliedstaaten herausbilden würde.

Die hohe Relevanz des Internet für eine Vielzahl gesellschaftlicher Bereiche und letztlich für die öffentliche Ordnung insgesamt unterstreicht, dass die transatlantische Cyberpartnerschaft transnational verankert werden muss, wenn sie langfristig stabil sein will. Bürger auf beiden Seiten des Atlantiks wurden für die Kehrseite der Digitalisierung sensibilisiert, und Forderungen nach einer Renationalisierung von Kommunikationsstrukturen ernten weithin lauten Beifall. Wenn dieser gefährlichen Entwicklung begegnet werden soll, bedarf es einer großangelegten Transparenzinitiative. Es ist unerlässlich, umfassend über die Praktiken der US-amerikanischen und der europäischen Nachrichtendienste zu informieren und öffentlich nachvollziehbar zu machen, dass auf Transparenz nicht verzichtet werden kann. Alles andere droht das für die Demokratie konstitutive Vertrauen zwischen Regierungen und Bürgern zu unterminieren und damit einen untragbar hohen Preis zu fordern.

Des Weiteren muss sich die Erkenntnis durchsetzen, dass die drei großen Themen Netzsicherheit, Datenschutz und Internet Governance zusammen verstanden werden müssen. Viel zu häufig werden die drei Themen unabhängig voneinander und ohne angemessene Einsicht in ihre wechselseitige Verschränkung behandelt. Es wird keine Sicherheit im Internet geben, wenn wichtige Staaten wie die Türkei, Brasilien, Indien oder Südafrika nicht in die Analyse der Probleme und die Suche nach Lösungen innerhalb der Internet Governance eingebunden werden. Das ist mit Staaten

wie Russland und China schwieriger zu bewerkstelligen, aber ebenfalls zwingend notwendig. Abschreckung allein schafft keine Sicherheit, genauso wenig wie die alleinige Konzentration auf Datenschutzrecht eine substantielle Datenpolitik hervorbringt.

Außerordentlich wichtig ist es auch zu begreifen, dass die Frage nach der Rolle des Staates in den verschiedenen Bereichen der Regulierung des Internet von Politikfeld zu Politikfeld unterschiedlich beantwortet werden muss. Die globalisierte Welt basiert auf der grenzüberschreitenden Digitalisierung von Infrastrukturen, von Wertschöpfungsketten und von Lebenswelten. Beim Schutz kritischer Infrastrukturen muss der Staat aus Sicherheitsgründen künftig eine größere Rolle einnehmen als in Fragen der wirtschaftlichen und technischen Entwicklung von Wertschöpfungsketten. Hier sind zuerst einmal die Privaten und eigenständige Koordinierungsprozesse in Multistakeholder-Foren gefordert. In der Regulierung gesellschaftlicher Lebenswelten und für alle sozialen Netzwerke sollte zudem gelten, dass staatliche Interventionen nur unter äußerst eng gefassten Bedingungen akzeptabel sind.

Die enge Verbindung der drei großen Themen Cybersicherheit, Internet Governance und Datenschutz sollte sich auf der administrativen Ebene in ein besseres Verständnis der engen Konsultation übersetzen. Stattfinden muss diese zwischen den verschiedenen zuständigen Generaldirektoraten der Europäischen Kommission sowie im Generalsekretariat des Ministerrates und in den zuständigen Fachabteilungen der Innen-, Verteidigungs-, Wirtschafts- und Justizministerien auf beiden Seiten des Atlantiks. In den USA hatte man bereits 2009 die Stelle eines Cyberkoordinators im State Department geschaffen. Ein vergleichbarer Schritt auf EU-Ebene steht noch aus. Zudem ist es unbedingt erforderlich, dass der transatlantische Gesetzgeberdialog in Fragen von Cybersicherheit, Internet Governance und Datennutzung über das bisherige Maß hinaus intensiviert wird und zivilgesellschaftliche Akteure stärker daran beteiligt werden. In der Cybersicherheit, der Internet Governance und im Datenschutz sollte jede Koordinierungsinstanz regelmäßig zivilgesellschaftliches sowie wissenschaftliches Problembewusstsein und -wissen einbinden. Nur so wird sich langfristig eine stabile transatlantische Cyberpartnerschaft etablieren lassen, die auf einem transatlantisch sowie transnational geteilten Wertefundament aufbaut.

Abkürzungsverzeichnis

ACTA	Anti-Counterfeiting Trade Agreement
BDI	Bundesverband der Deutschen Industrie
BMI	Bundesministerium des Innern
BRIC	Brasilien, Russland, Indien und China
BSI	Bundesamt für Sicherheit in der Informationstechnik (Bonn)
CDC SC	Cyber Defence Coordination and Support Center
CDMB	Cyber Defence Management Board
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Coordination des Normes Électriques
CIA	Central Intelligence Agency (USA)
CSCG	Cyber Security Coordination Group
CSIS	Center for Strategic and International Studies (Washington, D.C.)
DPPC	Defence Policy and Planning Committee
EC3	European Cybercrime Centre
EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency
EP	Europäisches Parlament
EP3R	European Public-Private Partnership for Resilience
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EUISS	European Union Institute for Security Studies (Paris)
FCC	Federal Communications Commission (USA)
FISA	Foreign Intelligence Surveillance Act
FISAA	Foreign Intelligence Surveillance Amendments Act
G8	Gruppe der Acht (die sieben führenden westlichen Industriestaaten plus Russland)
GCHQ	Government Communications Headquarters (GB)
IBSA	India, Brazil and South Africa Dialogue Forum
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
ISDS	Investor-State Dispute Settlement
ISOC	Internet Society
IT	Informationstechnologie
ITR	International Telecommunication Regulations
ITU	International Telecommunication Union
Nato	North Atlantic Treaty Organization
Nato C3B	Nato Consultation, Command and Control Board
NCIRC	Nato Computer Incident Response Capability
NIS	Netz- und Informationssicherheit
NRO	National Reconnaissance Office (USA)
NSA	National Security Agency (USA)
OECD	Organisation for Economic Co-operation and Development
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa

PEN	Poets, Essayists, Novelists
PNR	Passenger Name Record
SCS	Special Collection Service
TDL	Trust in Digital Life
TFTP	Terrorist Finance Tracking Program
TPP	Trans-Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
USSTRATCOM	United States Strategic Command
VN	Vereinte Nationen
VSBM	Vertrauens- und sicherheitsbildende Maßnahmen
WCIT	World Conference on International Telecommunications
WGIG	Working Group on Internet Governance
WSIS	World Summit on the Information Society

Lektüreempfehlungen

Annegret Bendiek
Kritische Infrastrukturen, Cybersicherheit, Datenschutz. Die EU schlägt Pflöcke für digitale Standortpolitik ein
SWP-Aktuell 35/2013, Juni 2013,
<www.swp-berlin.org/fileadmin/contents/products/aktuell/2013A35_bdk.pdf>

Annegret Bendiek
Europäische Cybersicherheitspolitik
SWP-Studie 15/2012, Juli 2012,
<www.swp-berlin.org/fileadmin/contents/products/studien/2012_S15_bdk.pdf>

Daniela Kietz/Johannes Thimm
Zwischen Überwachung und Aufklärung. Die amerikanische Debatte und die europäische Reaktion auf die Praxis der NSA
SWP-Aktuell 51/2013, August 2013,
<www.swp-berlin.org/fileadmin/contents/products/aktuell/2013A51_ktz_tmm.pdf>